International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2494-9150 Vol-02, Issue 01, APR 2016.

Digital Image Sharing and Removing the Transmission Risk Problem by Using the Diverse Image Media

[1]Shradha S. Rathod, [2]Dr. D. V. Jadhav,
[1]PG Student, [2]Principal, [1,2]TSSM's Bhivrabai Sawant College of Engg. & Research, Pune, Maharashtra, India.
[1]rathodshraddha27@gmail.com, [2]dvjadhao@yahoo.com

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. 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). The NVSS scheme uses the different carrier media to protect the secrete data. The proposed *(n, n)*- NVSS can share one digital secret image over *n – 1* arbitrary selected natural images (natural shares) and one noise like share. The natural share can be photos or a hand painted pictures. The NVSS scheme shares secret images via various carrier media to protect the secret and the participants during the transmission phase. The system proposes the possible ways to hide the noise like share to reduce the transmission risk problem for the share.

***Keywords* — *Data Hiding, Extended visual cryptography scheme, Image sharing, Natural shares, Transmission risk, Visual secrete sharing scheme*.**

I. INTRODUCTION

A technique that encrypts a secret image into *n* shares, with each participant holding one or more shares is visual cryptography (VC). Anybody who holds fewer than *n* shares cannot reveal any information about the final secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human eyes.

Secrete image can be of various types: photographs, handwritten documents, images, and others. It is very important to secure the data in computer aided environment. Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents, but they will suffer from two drawbacks: first, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted.

The existing VSS scheme still must be investigated for reducing the transmission risk problem. The proposed scheme uses diverse media for sharing the digital images. The NVSS scheme uses diverse media as a carrier; hence it has possible scenarios for sharing secrete images.

Previous research into the Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme provided some effective solutions to cope with the management issue [1-2]. The shares contain many noise-like pixels or display low quality images. Such shares are easy to detect by the naked eye, and participants who transmit the share can easily lead to suspicion by others. By adopting steganography techniques, secret images can be concealed in cover images that are halftone gray images and true-color images [5-6]. However, the stego-images still can be detected by steganalysis methods [7]. Therefore the existing VSS schemes still must be investigated for reducing the transmission risk problem for carriers and shares. A method for reducing the transmission risk is an important issue in VSS schemes.

In this paper, efficient encryption/decryption algorithms for the (*n, n*) -NVSS scheme is developed. 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.

A. Classification of VSS Scheme

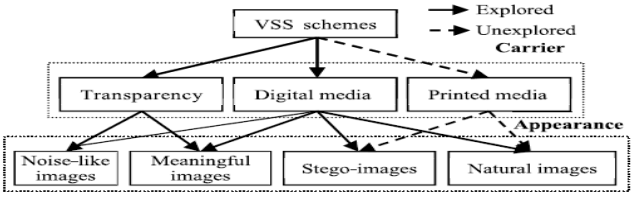

Fig.1: Classification of VSS Scheme

Fig.1 shows the classification of VSS scheme from carriers' viewpoint. This system proposes only transparencies or digital media as carriers for a VSS scheme.

II. THE PROPOSED SCHEME

In the NVSS scheme, the natural shares can be gray or color photographs of scenery, family activities, or even fly sheets, bookmarks, hand-painted pictures, web images, photographs. The natural shares can be in digital or printed form. The encryption process only extracts features from the natural shares; it does not alter the natural shares. The innocuous natural shares can be delivered by participants who are involved in the NVSS scheme, by the owners of the photographs, or via public Internet. Because the natural shares are not altered, it is likely that they will not arouse suspicion during transmission. Even if the natural shares are intercepted, it will not be possible to verify that there is any hidden information in the images before reaching the decryption threshold. In such a scenario, the transmission of the innocuous natural shares is more secure than the transmission of shares in another form, such as noise-like or meaningful shares. Another share, which is generated by the secret image and features that are extracted from *n-1* natural shares, can be hidden behind other media and then delivered by a well-disciplined person or via a high-security transmission channel.

III. ENCRYPTION PROCESS OF NVSS SCHEME

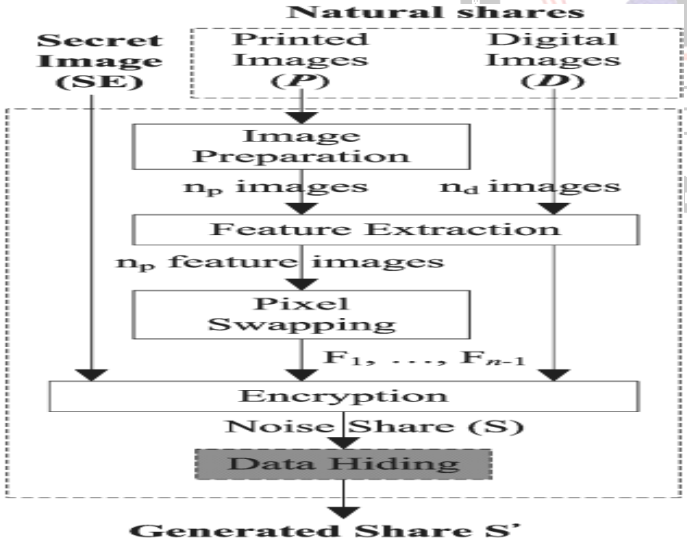

Fig.2: Encryption Process of NVSS Scheme

Fig. 2 shows the encryption process of proposed (*n, n*)-NVSS scheme, $n \geq 2$, includes two main phases; feature extraction and encryption.

A. Image Preparation and Pixel Swapping

The image preparation and pixel sapping processes are used for pre-processing printed images and for post-processing the feature matrices that are extracted from the printed images. The printed images were selected for sharing secret images, but the contents of the printed images must be acquired by computational devices and then be transformed into digital data.

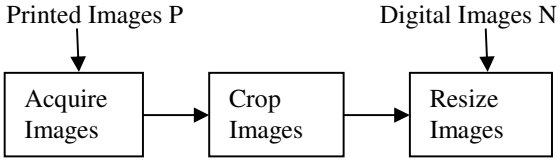

Fig.3: Flow of Image Preparation Process

The suggested flow of the image preparation process is shown in Fig. 3. In the first step, the contents of the printed images can be acquired by popular electronics devices, such as digital scanners and digital cameras. To reduce the difference in the content of the acquired images between the encryption and decryption processes, the type of the acquisition devices and the parameter setting (e.g., resolution, image size) of the device should be the same or similar in both processes. The next step is to crop the extra images. Finally, the images are resized so they have the same dimensions as the natural shares.

B. Feature Extraction

Feature extraction is carried by Binarization of the natural shares. Binarization performed by calculated with respect to median value of natural shares. With the binarization result the stabilization process is done. Stabilization process is used to stabilize the number of black and white pixels of an extracted feature image in each block. The process ensures that the number of black and white pixels in the block is equal. The chaos process is used to eliminate the texture that may appear on the extracted feature images and generated shares.

1] Algorithm of feature Extraction:

1. Divide N into blocks with b x b pixels.
2. For each block repeat step 3- 4.
3. $\forall\ x_1 \leq x \leq x_b$, $y_1 \leq y \leq y_b$, calculate $H^{x,y}$ by equation 1.
4. Calculate M.
5. $\forall\ x_1 \leq x \leq x_b$, $y_1 \leq y \leq y_b$ determine $f^{x,y}$ by equation 2.
6. Calculate Q_s by equation 3.
7. Randomly select Q_s pixels where $f^{x,y}$=1 and $H^{x,y}$ =M. Let $f^{x,y}$ 0. ←
8. Calculate Q_c by equation 4.
9. Randomly select Q_c candidate pixels where $f^{x,y}$ =1.
10. Randomly select Q_c candidate pixels where $f^{x,y}$ =0.
11. After all values of $f^{x,y}$ that where selected in step 9 and 10.
12. Output F.

C. Encryption Process

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

[2] Algorithm of Encryption/ Decryption Process

1. Initialize the random number generator G by the seed p.
2. n $n_p + n_\alpha \leftarrow 1$.
3. $\forall 1 \le \alpha < n, \forall \varphi \in \{R, G, B\}, FI_{\alpha,\varphi} \quad 0.$ ←
4. $\forall 1 \le \alpha < n, \forall \varphi \in \{R, G, B\}, \forall 0 \le i \le 7$, repeat step 5 and 6.
5. Call procedure FE (N_α, b, P_{noise},F).
6. $\forall(x, y)$, x Є [1, w], yЄ [1, h], $p_{\alpha,\varphi}^{x,y} \leftarrow f^{x,y}$ x2^i.
7. If $n_p = 0$ then go to step 12.
8. $\forall 1 \le \alpha \le n_p$, repeat step 9-11.
9. Randomly selects (x_1, y_1), x_1 Є [1, w], y_1 Є [1, h].
10. Randomly selects (x_2, y_2), x_2 Є [1, w], y_2 Є [1,h].
11. $\forall\varphi$ Є {R, G, B}, exchange values of $p_{\alpha,\varphi}^{x1,y1}$ and $p_{\alpha,\varphi}^{x2,y2}$.
12. $\forall\varphi$Є{R,G,B}
13. $\check{S}_\varphi \quad S_\varphi \otimes \leftarrow FI_{1,\varphi} \otimes \dots \otimes FI_{n-1,\varphi}$
14. Output Š

D.Data Hiding

In this section 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 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. Here the focus is on how to hide the share in printed media using QR code technology.

The QR code is a two-dimensional code first designed for the automotive industry. The QR code which encodes meaningful information in both dimensions and in the vertical and horizontal directions, can carry up to several hundred times amount of data carried by barcodes. The code is printed on physical material and can be read and decode by various devices, such as barcode readers and smart phones. Today, the QR code is widely used in daily life, and is widely visible, on the surface of products, in commercial catalogs and flyers, in electronic media, and elsewhere. It is this ubiquitous nature of the QR code that makes it suitable for use as a carrier of secret communications.

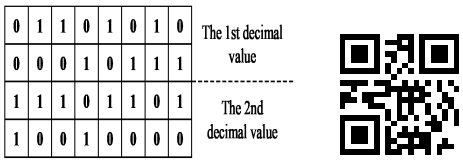

Fig.4: An example of the feature matrix to the QR code encoding: (a) the feature matrix, (b) the corresponding QR code of the matrix

The amount of data that can be stored in the QR code symbol depends on the data type (e.g., numeric, alphanumeric, byte/binary, Kanji), versions and error correction level. In this paper, we will pretend the noise-like share as the numeric type of the QR code. The encoding process consists of two steps: First, transform pixels on the share into binary values and represent the values in a decimal format. In this step, 16 binary feature bits are converted into a 5-digit decimal value, which ranges from 0 to 65,535. Second, we encode the decimal values into QR code format.

[1] Algorithm of Share Hiding

1. C_s h x w; $C_r \leftarrow [C_s/C_H] \leftarrow F_{QR}$ Null string ←
2. Vectorize F to bit-string S_F .
3. S_t removes ← (S_F, C_r).
4. If H(S_t) < C_r/2 then S_b 0. ←
5. Append S_b for F_{QR}.
6. If $S_F \neq$ null string then goto step 3.
7. S_{QR} Null string.
8. Convert h, w, C_r to string and append these string to S_{QR}.
9. S_t Remove ← (F_{QR}. 16).
10. num $\sum_{0 \le i \le 15} S_{ti} \times 2^i$.
11. Convert num to string and append the string to S_{QR}.
12. If $F_{QR} \neq$ null string then goto step 9.
13. Output S_{QR}.

IV. DECRYPTION PROCESS OF NVSS SCHEME

Fig. 3 shows the decryption process of NVSS scheme. When all n shares are received, the decryption end extracts n-1 feature images from all natural shares S' to obtain the recovered image as shown in figure.

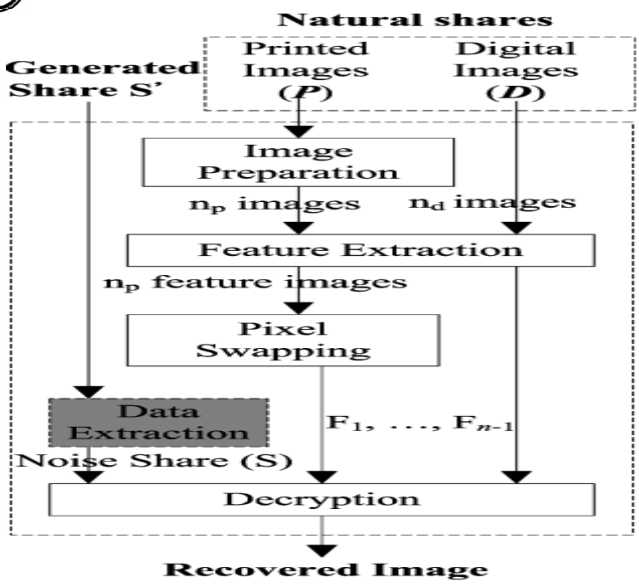

Fig. 5: Decryption Process of NVSS scheme

By repeating the reversal process of encryption process to predict the secret image. Again feature extraction and pixel swapping performed to predict the secret image.

[4] Algorithm of Share Extraction

1. Retrieve h, w and C_r from S_{QR}.
2. F_{QR} ← Null string.
3. S remove (S_{QR}, 5).
4. Num ← str2int(S).
5. ∀ 0 ≤ i ≤ 15, append C_r, consecutive bits with value num_i to F_{QR}.
6. If S_{QR} ≠ null string then go to step 3.
7. Transform vector F_{QR} to matrix F with h x w entries.
8. Output F.

V. EXPERIMENTAL RESULTS

The image preparation of the printed image as shown in fig. 6, contains the three steps acquire image, crop image and resize the image the resized image is shown in fig. 7 and filtered the printed image as shown in fig. 8.

Fig. 6: Printed Image

Fig. 7: Cropped and Resized image

Fig. 8: Filtered Printed Image

The digital image is taken as shown in fig, 9, then digital image is filtered as shown in fig. 10.

The filtered Image is Binarized as shown in fig, 11, then the Binarized image is stabilized by stabilizing the white and black pixels randomly as shown in fig. 12. After stabilization process he Chaos process is done Chaos process is used to eliminate the texture of the image as shown in fig. 13.

Fig. 9: Digital Image

Fig. 10: Filtered Digital Image

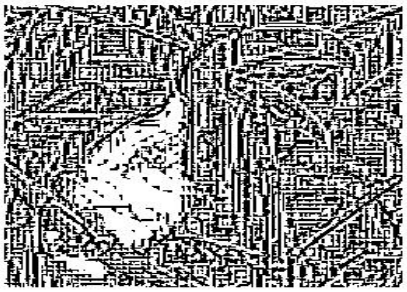

Fig. 11: Binarization of Digital Image

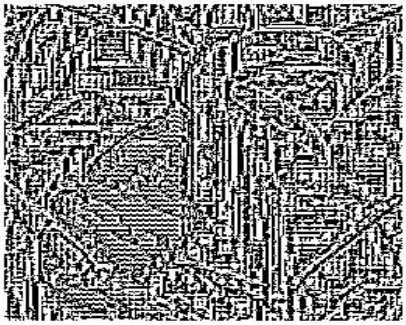

Fig. 12: Stabilization of digital image

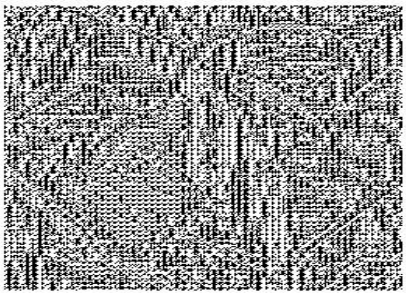

Fig. 13 Chaos process of Digital Image

V. CONCLUSION

In this work NVSS scheme that can share a digital image using diverse image media. The media that include n-1 randomly chosen images are unaltered in the encryption phase. The NVSS scheme uses the noise like share for protecting the secrete data.

This study provides the four contributions. First is to share the data via different carriers in VSS scheme. Second, successfully introduce hand printed images for image-sharing schemes. Third, used the unaltered images as shares. Fourth, used the method to store the noise like shares as the QR code.

Compared with the existing VSS schemes, the proposed NVSS scheme can reduce the transmission risk and provide the highest level of user friendliness, both for shares and participants.

REFERENCES

1] 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.

2] 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.

3] 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.

4] 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.

5] 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.

6] 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.

7] A. Nissar and A. H. Mir, "Classification of steganalysis techniques: A study," Digit. Signal Process., vol. 20, no. 6, pp. 1758–1770, Dec. 2010.

8] Guo, C. C. Chang, and C. Qin, "A multi-threshold secret image sharing scheme based on MSP," Pattern Recognit. Lett., vol. 33, no. 12, pp. 1594–1600, Sep. 2012.

9] P. L. Chiu, K. H. Lee, K. W. Peng, and S. Y. Cheng, "A new color image sharing scheme with natural shadows," in Proc. 10th WCICA, Beijing, China, Jul. 2012, pp. 4568–4573.

10] J. Fridrich, M. Golijan, and D. Soukal, "Perturbed quantization steganography with wet papers codes," in Proc. Workshop Multimedia Sec. Magdeburg, Germany, Sep. 2004, pp. 4-15.