IJIR

INTERNATIONAL JOURNAL OF INNOVATION RESEARCH

Available Online at http://www.journalijir.com

Vol. 4, Issue, 5, pp. 79-82, May, 2016

ISSN: 2249-1465

Research Article

DIGITAL IMAGE SHARING AND REMOVING THE TRANSMISSION RISK PROBLEM BY USING THE DIVERSE IMAGE MEDIA

Shradha S. Rathod and Dr. D. V. Jadhav

E & TC Engineering Department, TSSM's Bhivrabai Sawant College of Engg. & Research, Pune, India

ARTICLE INFO

Received 10th February, 2015
Received in revised form 13th March, 2016 Accepted 20th April, 2016
Published online 28th May, 2016

Keywords:

Data Hiding; Extended visual cryptography scheme; Image sharing; Natural shares; Transmission risk; Visual secrete sharing scheme.

ABSTRACT

Sharing the sensitive information or data over a network conventional visual secrete sharing scheme is used. The conventional VSS scheme hides the secrete information in different shares. The shares can be noise-like pixels or meaningful images. The visual secrete sharing scheme has major problem that it suffers from a transmission risk problem for the secrete data and there is a possibility that the hackers may get the information. To overcome this problem the natural visual secrete sharing scheme (NVSS) is used. The NVSS scheme uses the natural images like paintings, photographs, hand painted pictures etc. as natural shares. As the NVSS scheme uses natural shares it reduces the transmission risk problem at a certain limit. The NVSS scheme uses different carrier media to transmit the information securely. The NVSS scheme is hides the secrete image by using the other natural shares. The NVSS system gives the solution for transmission risk problem and securely hides information.

INTRODUCTION

The proposed technique that divides a secret image into *n* shares, at the time of sharing the data to the participants, each participants holds one or more share which is known as visual cryptography (VC). If anyone have less than *n* shares, they cannot get the information about final secrete image.

The secrete images can be of various types such as printed images , photographs, hand written documents, printed images etc. It is very important to secure the data in a computer-aided environment.

In a VSS scheme the image is divided into different component images. Each pixel of the image component is divided into parts. If the pixel of image component is divided into two parts then it has one white and one black block.

The existing VSS scheme suffers from a transmission risk problem and there is a possibility that hackers may get the information about secrete image. To avoid this problem the NVSS scheme is used. The NVSS scheme transmits the secrete image securely through a network. The scheme combines one or two images to the secrete image, the images which are combined that are natural shares. NVSS scheme uses the different carrier media to protect the information.

The previous research into the Extended Visual Cryptography Scheme (EVCS) scheme solves the management problem at certain level [1-2]. The shares contain many noise-like pixels, and there must be possibility that the hacker gets the information and it is easy to detect the information by naked eye. Therefore the existing VSS scheme has some drawback that it has some transmission risk problem, still the research is going on.

In this paper, efficient encryption and decryption algorithms for the (*n*, *n*) -NVSS scheme is developed. The proposed algorithms are applicable to digital and printed media. And how to hide the generated share are also discussed in the proposed scheme. The proposed NVSS scheme has a high level of user friendly, reduces transmission risk and enhances the security of participants and shares.

The nvss scheme

In the NVSS scheme, the natural shares are photographs, family activities, bookmarks, hand-painted pictures, web images, Photographs etc. The natural shares are color photographs or gray. The natural shares are basically in digital or printed form. In the encryption process the information is hided.

*✉ ***Corresponding author:*** **Shradha S. Rathod**
E & TC Engineering Department, TSSM's Bhivrabai Sawant College of Engg. & Research, Pune, India

Encryption process of nvss scheme

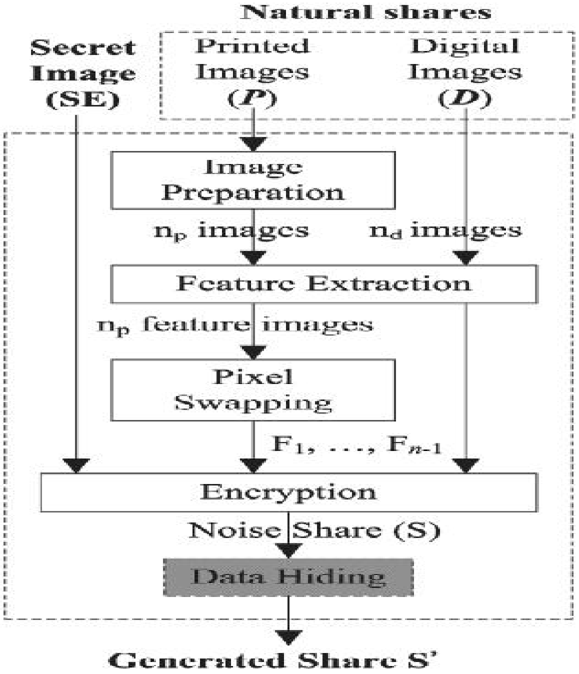


Fig. 1 Encryption Process of NVSS Scheme

Fig. 1 shows the encryption process of proposed (*n, n*)-NVSS scheme, *n* ≥ *2*, the encryption process of NVSS scheme has two main parts; feature extraction and encryption.

Image Preparation and Pixel Swapping

The image preparation is used for pre-processing and pixel swapping is used for post-processing the extracted image. The steps of image preparation is shown in Fig.2.

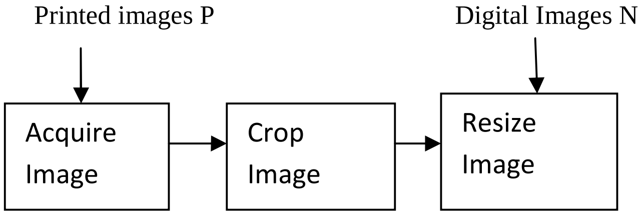


Fig.2 Steps of Image Preparation Process

Feature Extration

Feature extraction contains 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. The process ensures that the number of black and white pixels in block is equal. The chaos process is used to eliminate the texture of the images.

Encryption process

Before Encryption process pixel-swapping for printed image share performed which tolerance of the image distortion caused by the image preparation process.

Data Hiding

The Quick-Response code is used to hide the information, so that no one can get the secrete information easily.

Decryption process of nvss scheme

Fig. 3 shows the decryption process of NVSS scheme. The secrete data can be recovered by using the generated shares.

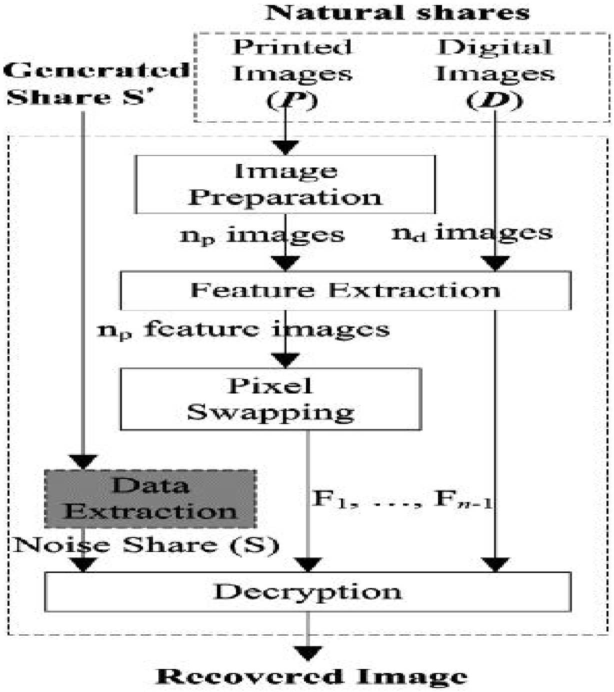
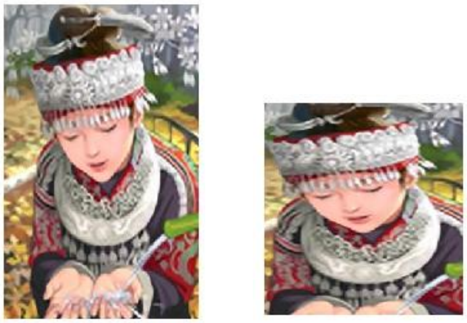


Fig. 3 Decryption Process of NVSS scheme

By reversing the encryption process secrete image is formed. Again feature extraction and pixel swapping performed to get the secret image.

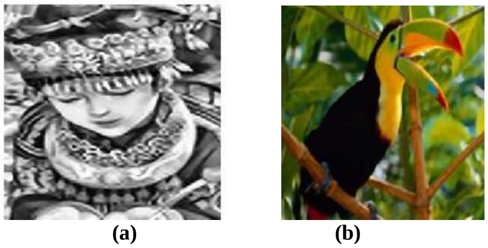
experiments and results

The image preparation of the printed image as shown in Fig. 4(a), contains the three steps acquire image, crop image and resize the image the resized image is shown in Fig. 4(b) and filtered the printed image as shown in Fig. 5(a).



(a) **(b)**

Fig. 4 **(a)** Printed Image **(b)** Cropped & Resized Image



(a) **(b)**

Fig. 5 (a) Filtered Printed Image (b) Digital Image

The digital image is taken as shown in Fig, 5(b), then digital image is filtered as shown in Fig. 6. Then the Binarized image is as shown in Fig. 7(a), after that the Binarized image is stabilized by stabilizing the white and black pixels randomly as shown in Fig. 7(b). After stabilization process he Chaos process is done Chaos process is used to eliminate the texture of the image as shown in Fig. 8(a).

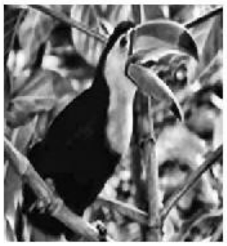
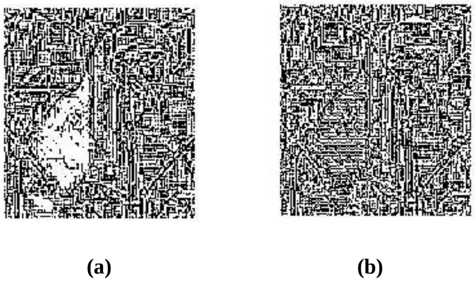


Fig. 6 Filtered Digital Image

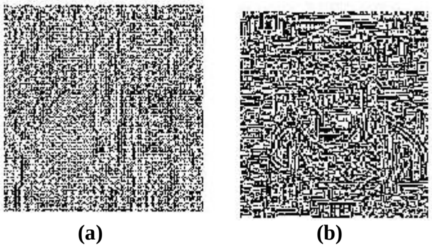


(a) **(b)**

Fig. 7 (a) Binarization of digital Image (b) Stabilization of Digital Image

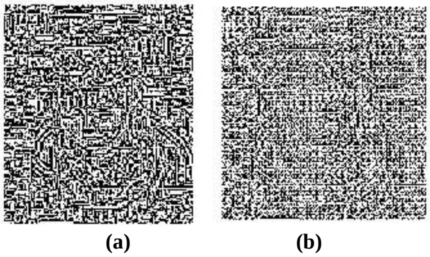
The binarization of printed image is shown in Fig. 8(b), after that the binarized image is stabilized using stabilization process shown in Fig. 9(a), the chaos process is done shown in Fig. 9(b). The pixel swapping process is shown in Fig. 10(a). Then the extracted image is formed as shown in Fig. 10(a).Then the encrypted image is formed as shown in Fig. 11(b).

The secrete image is recovered from the generated shares as shown in Fig. 12.



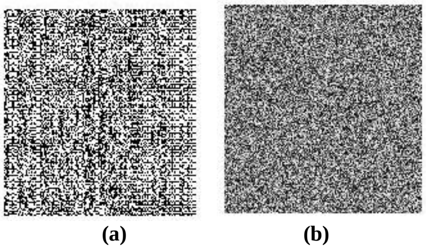
(a) **(b)**

Fig. 8 (a) Chaos Process of Digital Image (b) Binarization of printed Image



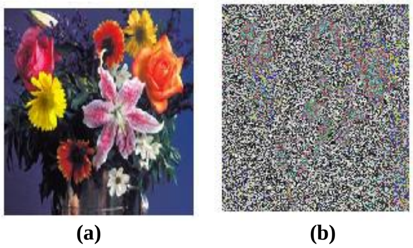
(a) **(b)**

Fig. 9 (a) Stabilization of printed Image (b) Chaos Process of Printed Image



(a) **(b)**

Fig. 10 (a) Pixel Swapping of Image (b) Feature Extraction of printed Image



(a) **(b)**

Fig. 11 (a) Secrete Image (b) Encrypted Image

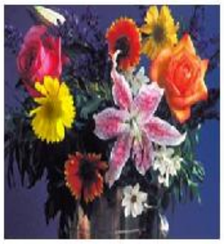


Fig. 12 Decrypted Image

Acknowledegement

I would like to thank all people who help me in different way. Especially, I am thankful to my guide Dr. D. V. Jadhav and P.G. Co-ordinator Prof. Pansambal B. H. for their continuous support and guidance in my work. Also, I would like to thank H.O.D. of E & TC (Signal Processing)Engg. Department,Prof. Pawar D. B. for motivating me. Lastly, I thank to EPGPEX who have given opportunity to present my paper.

CONCLUSIONS

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. Secures the data from hackers and the recovered image is same as the original image.

This proposed system gives 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 problem and the system is user friendly, both for participants and shares.

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.
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.

****