ISSN:0975-9646
Mayuri Sonkusare et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3784-3786

Analysis of Digital Image Sharing By Diverse Image Media

[1]Mayuri Sonkusare, [2]Prof. Nitin Janwe
[1,2]*Computer Science and Engineering Department*

Abstract: A natural-image-based VSS scheme (NVSS scheme) that shares secret images. A natural-image-based secret image sharing scheme (NSISS) that can share a color secret image over n - 1 arbitrary natural images and one noise-like share image. Instead of altering the contents of the natural images, the encryption process extracts feature images from each natural image. In order to protect the secret image from transmission phase. (n, n) - NVSS scheme shared secret image over n-1 natural share. The natural shares will be digital image and printed image. By extracting the features of natural shares we can prepare noise-like share. After that encryption carried out with noise-like share and secret image. Propose possible ways to hide the noise like share to reduce the transmission risk problem for the share.

In this paper Initially Feature Extraction process has been performed for Natural Shares. Here Digital image and Printed image have been used as Natural Shares. With that extracted features secret image will be encrypted by (n, n) - NVSS scheme where process carried by (n-1) natural shares. This Encrypted result will be hided using Share-Hiding Algorithm where generated the QR code. In the Recovering of the secret image will be done by Share Extraction Algorithm and also decryption algorithm. Finally the secret image with all pixels has been obtained. This proposed possible ways to hide the noise like share to reduce the transmission risk problem for the share.

Keywords: Visual secret sharing scheme, extended visual cryptography scheme, natural images, transmission risk.

1. INTRODUCTION

Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images.a block-based transformation algorithm based on the combination of image transformation and a well known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. Due to large data size and real time constrains, algorithms that are good for textual data may not be suitable for multimedia data.

Encryption is the process of transforming the information to insure its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. As a result, different security techniques have been used to provide the required protection. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems to encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image types.

Module Description:

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. Resize the cropped image with predicted size.

Feature Extraction

Feature Extraction is carried by Binarization of the natural share. Binarization performed by calculated with respect to the median value 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. The process ensures that 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.

Encryption:

Before Encryption process pixels-swapping for printed image share performed 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.

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. The string can be encoded to the QR code (a stego-share) by QR code generators.

Decryption:

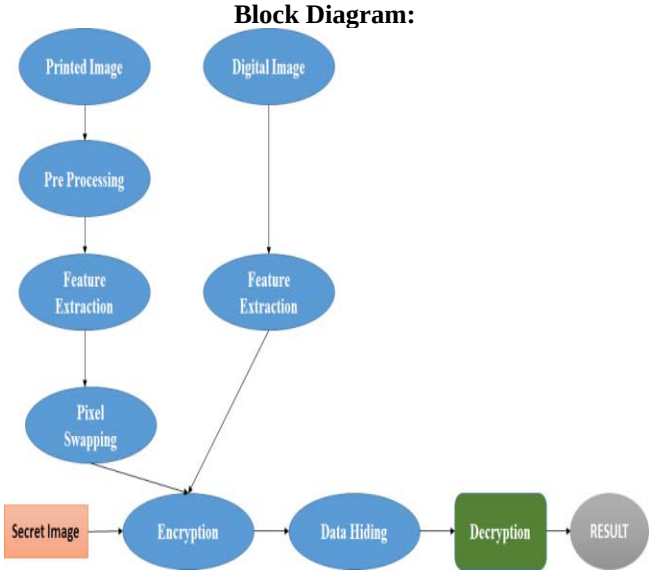
By repeating the reversal process of encryption process to predict the secret image. Again feature extraction and pixel swapping performed to predict the secret image.

2. RESULTS AND DISCUSSION

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

Feature extraction has been performed for two natural shares, so as the natural share's pixels are more efficiently compressed. This 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 performed with the 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 performed and decryption algorithm applied to recover the Secret image.

Block Diagram:



Advantage:

- In order to implement the natural share by feature extraction and pixel swapping can effectively improve the performance of encryption process.
- To combine the QR code in the step of Data Hiding can make it suitable for use as a carrier of secret communications.

Applications:

- Secure Web browsing using Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols, the use of encryption may be transparent to users.
- Encrypting entity needs to share the key with a separate decrypting entity, the key must be transported to the decrypting entity in a secure manner.
- It also applied in the field of ecology, biometrics and medical applications.

COMPARISION

Existing System	Proposed System
1. In the existing provided unsecure result. 2. Storage and transmission of the shares requires an amount of storage and bandwidth resources equivalent to the size of the secret times the number of shares. 3. Not performed data hiding process so that not able to perform efficient result.	1. In the proposed approach can process with natural shares and Secret image so can able to achieve more secured manner. 2. In this process storage resources not much as in existing because of performed feature extraction. 3. To combine the QR code in the step of Data Hiding can make it suitable for use as a carrier of secret communications.

CONCLUSIONS

In this paper a VSS scheme, (n, n)-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. 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.

FUTURE WORK:

In enhanced system can segment the secret image and will perform the encryption process for all segmented regions, the same process will inversely perform in decryption, in order to achieve the efficient transformation of secret images.

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] 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 Comput. 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," Digit. Signal Process., vol. 21, no. 6, pp. 734–745, Dec. 2011.