Secure Data Transmission by Images

Mr. Rishabh Badnore [1], Mr. Tejas Pote [2], Mr. Raj Gaikwad [3], Mr. Umesh Chaudhari [4] , Mr. A. N. Bandal [5]

[1,2,3,4,5]*Department of Computer Engineering, STES' SINHGAD INSTITUTE OF TECHNOLOGY, Lonavala*
Savitribai Phule Pune University, Maharashtra, India

***

Abstract: *This computerized do in digital word data sharing is crossable techniques to contribution or transfer data one location to another location. Data sharing means transfer classified details from source to destination. In existing system has different techniques used to transfer data buts not secure. In recent year digital image sharing is secure and hard to extract techniques. But in image processing you add some data or not then disturb image and it's easily to detect file has changes or corrupted. Because it's add or remove noise of system. To avoid this problem we implement visual secret sharing (VSS) schemes for merge multiple images parts. These images are hide to cover images for display normal images like image share. The natural parts can be photos or painted images in digital form or in printed form. The noise part is generate based on natural images and secrete images huge reduces the transmission problem. We also give possible ways to hide the noise like share to reduce the transmission problem for the share. Experimental results point to that the proposed approach is an outstanding solution for solving the transmission risk problem for the VSS schemes.*

Key Words: Visual secret sharing scheme; extended visual cryptography scheme; Natural images; Transmission risk.

1. Introduction:

In security domain main motto is securely stored data or securely transfer data form source to destination. In security domain has cryptography used to encryption and decryption of things. Data convert into cryptography format to its hard read normal user. Visual cryptography concept proposed to Naor and Shamir to hide secret information [2].

In digital image sharing before transfer data convert into cryptography format in using different techniques. Digital images has generate to different color shade. In image processing has three channel are important Red, green, Blue. Which has create a different combinational colors. In prepossessing structure calculate all color RGB values to perform operation.

Image processing has modify image to operation which has loss our pixel or color shade. Means it disturb to original images and adding with noise. So it's called as noisy images. Which can easily see that some changes are available in images? Pixel expansion problem are generated to above things. Which has losing our image original pixel in processing of image [2]? In display has reduce quality of image and pixel to VC. To reduce brightness each calculate decrease quality of images [1].

Conventional VC schemes have focused on the encrypting/decrypting of secret images printed on transparencies [1]. Visual cryptography encryption has different algorithm are use like AES, DES, ECC etc. which algorithm you encrypted image of hidden data which are not recover because pixel losing possibility is high. In pixel expansion problem has increase in this algorithm.

According InKoo Kang [4], visual information pixel (VIP) synchronization and error diffusion to attain a color visual cryptography encryption method that produces meaningful color shares with high visual quality. That can be used for implemented method for synchronized images pixel. In visual cryptography has apply to n share concept. Same Images has adding data and merging into one image which has display to two different images.

In this study, we introduce a VSS scheme or natural image based VSS scheme to minimize the interception risk during transmission phase. Usual VSS schemes use a unity carrier or digital image for sharing images which confines the practicality of VSS schemes. In the given process we explore the possibility of using diverse media for sharing digital images. The carrier media use in this process contains digital images, printed images, hand painted picture and so-on.

EVCS can also be treated as a method of steganography. One situation of the applications of EVCS is to avoid the tradition inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected [5]. LSB steganography can easily hide textual data. In this techniques hide information in last bit. Which depend upon byte conversion code?

In this paper, we expand efficient encryption/decryption algorithms for the (n, n) -NVSS scheme. The projected algorithms are relevant to digital and printed media. The possible ways to conceal the generated share are also discussed. The NVSS project not only has a high level of user responsiveness and manageability, but reduces transmission risk and enhances the security of contributor and segments.

1.1 Related Work:

In image processing, data handling is difficult task. Presented techniques has apply in images which hide sensitive data.

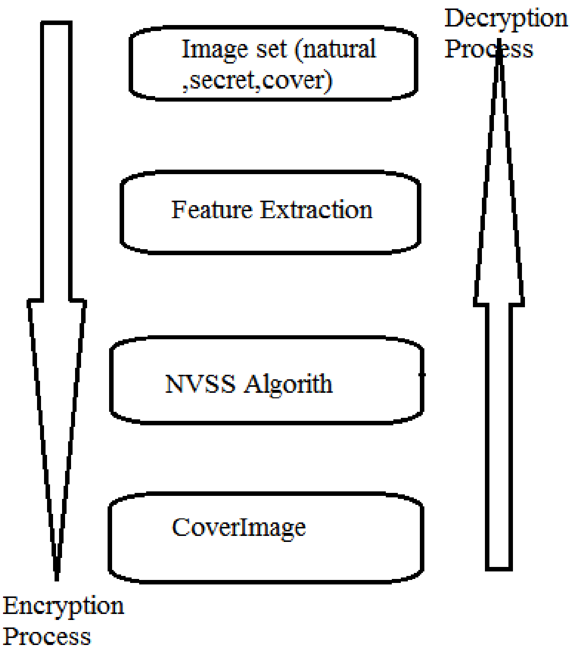


Fig1. System flow

To perform Natural image visual secret sharing algorithm has designed to encryption process which has transfer data performing operation to hide image. In image set are sort out in a feature extraction which can natural images, secret images and cover images to perform NVSS algorithm for encryption method.

In decryption process are inverse. First you extract cover image to remove image and getting xor noise image. These noise image process in XOR operation to getting secret image as you hide.

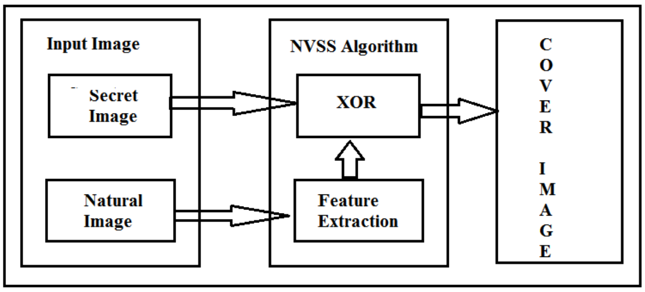


Fig2. Architecture

System input image share both images. It has contain single secret image and group of natural images and cover images. In natural images has getting feature extraction to generate combination merging image. Which merging image and hiding secret image perform xor operation to hiding image. To Implementing NVSS algorithm see the noise image which has getting cover of images to transfer a destination image. Its overall process is encryption process.

In visual cryptography has only one image so it does not generate merging image. These image has different combination so any user not attention of images. User can easily send secure information to destination. Steganography is the method of hiding information and making the message unseen. So, the concealed information and its carrier can be secluded. Steganography has been use to hide digital shares in VSS schemes. The shares in VSS schemes are fixed in cover images to make stego-images. Although the shares are covered totally and the stego-images have a elevated level of user friendliness, the communal information and the stego-images stay intercepted risks during the broadcast stage. Recently, Chiu et al. tried to share a secret image via customary images. This was a first effort to share images via usual images though, this work may undergo a problem the textures of the usual images could be disclosed on the share. Furthermore, printed images cannot be used for distributing images in the preceding scheme.

Presented study focuses only on with transparencies or digital media as carriers for a VSS scheme. The simplicity shares have either a noise-like or a meaningful form. The conservative noise-like shares are not gracious [2]; hence, researchers tried to improve the friendliness of VSS schemes for participant [3]. Normally, easy and significant coat images are added to noise-like shares for detection, making conventional VC schemes more friendly and convenient. Though, the EVCSs decrease the display quality of the recovered images. Research has focused on color and gray-level secret images to build up a user-friendly VSS scheme that adds cover up images into the meaningless shares [10]. To digital images share, VSS techniques use digital media as mover, which makes the form of the shares more variable and more user friendly [10]. Several investigated papers shows meaningful halftone shares [5] and emphasized the excellence of the shares extra than the class of the recovered images. These studies had grave side effects in terms of pixel expansion and deprived display excellence for the improved images, though the display quality of the shares was improved. Hence, researchers create a tradeoff between the quality of the shares, the quality of the recovered images, and the pixel growth of the images. In an additional research bough, researchers used steganography technique to secret images in wrap images [9]. Steganography is the method of hiding information and making the message unseen. So, the concealed information and its carrier can be secluded. Steganography has been use to hide digital shares in VSS schemes. The shares in VSS schemes are fixed in cover images to make stego-images. Although the shares are covered totally and the stego-images have an elevated level of user friendliness, the communal information and the stego-images stay intercepted risks during the broadcast stage. Recently, Chiu et al. tried to share a secret image via customary images. This was a first effort to share images via usual images though, this work may undergo a problem the textures of the usual images could be disclosed on the share. Furthermore, printed images cannot be used for distributing images in the preceding scheme. So far, distributing visual secret image via unchanged printed media leftovers an open problem. In this revise, we make an addition of the preceding work in to encourage its viability and discover the option for adopting the unaltered printed media as shares.

1.2 Techniques:

In secret image sharing has different algorithm are used.

1.2.1 Feature Extraction:

Image processing has perform to getting all history of images which has image color in rgb values, type and other details. In preprocessing concept getting 3 parts. Getting color module, grayscale conversion and edge detection.

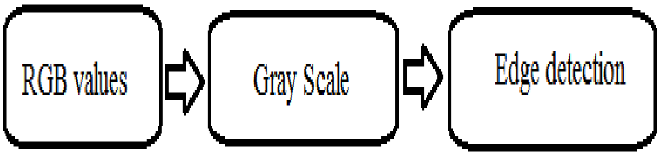


Fig1. Feature.

In feature stage calculating upload images detail like count of natural images, secret image detail and cover image detail are stored.

1.2.2 Blocking:

In cryptography process has get multiple natural images files for combining in parts. Consider User select two files then create a new file which has merging combinational files. These two files are divided in center of and merge in half-half images. First we calculate count of natural images and divide into height and weight of natural images.

$$n = count(Natural\ images)$$

$$x = \frac{nauralImage_{width}}{n}$$

$$y = nauralImage_{height}$$

$$image = crop\_image(x, y)$$

Where n=count of natural images.

X=new generated width

Y=new generated height

Image = new crop images with x,y position.

To generate more complexity user can upload multiple natural images. We are divide each image and getting subparts of images. Consider user upload 4 images then system generate 25%, 25%,25%,25% per image and merging each part generate 100% merging image.

1.2.3 Merging:

All natural divide into subparts like secret image height and width. These combination image are hiding to secret image. In hiding process we have implement steganography concept. These are apply under NVSS techniques.

1.2.4 NVSS:

A natural image visual secret has set of different algorithm.it has divide the natural images in different share. These every share are make to one image and hide the secret image behind natural image. The algorithm show in mathematical format.

1.3 Mathematical Module

The algorithm show in mathematical format.

A. Mathematical Module

$$Imag = \int_0^n secret\ imag + \int_0^n Natural\ imag \qquad (1)$$

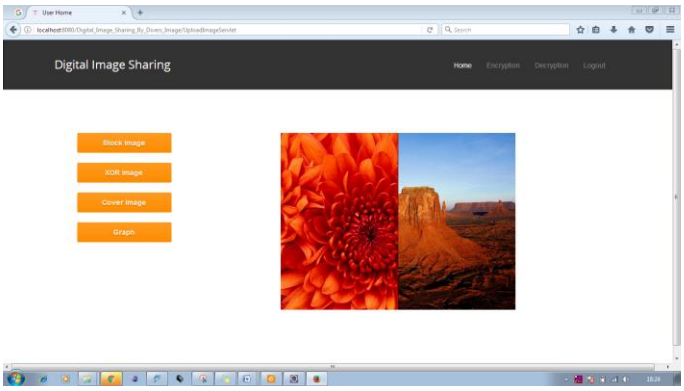
User has sets to secret and natural images sets.

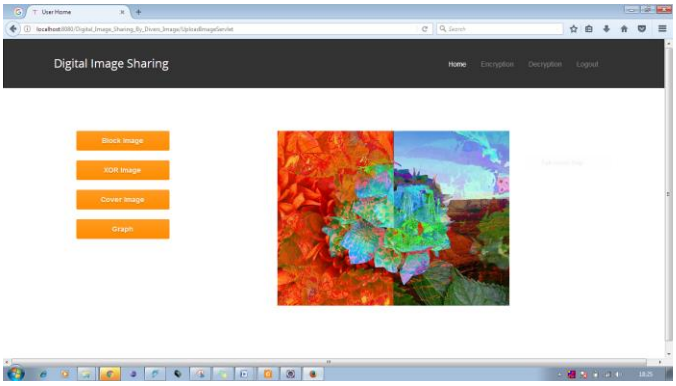
$$val(RGB)\ €\ Imag \qquad (2)$$

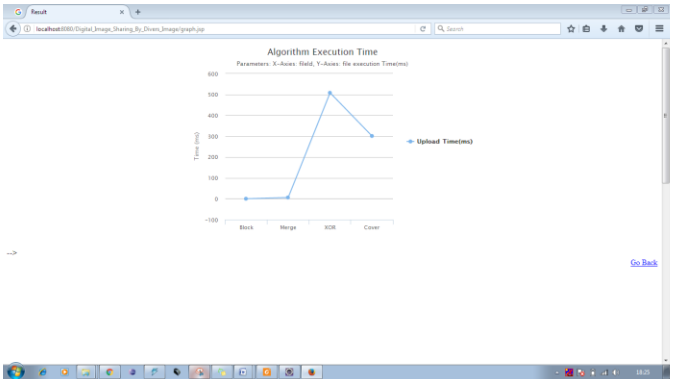
$$Output = cover \oplus Imag \qquad (3)$$

Final output generated by XOR operation using cover image and Image sets.

2. Implementation Result:







3. CONCLUSIONS:

The paper propose a VSS scheme, (n, n)-NVSS scheme, that can share a digital image using diverse image media. The media that include n1 arbitrarily selected images are unchanged in the encryption stage. Therefore, they are totally inoffensive. Despite of the number of participant n increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with obtainable VSS schemes, the projected NVSS scheme can efficiently decrease broadcast threat and give the maximum level of user sociability, for both shares and for participants. This revise provides four main contributions. First, this is the first effort to share images via heterogeneous carriers in a VSS scheme. Second, we productively set up hand-printed images for images-haring schemes. Third, this study proposes a practical concept and technique for using unchanged images as shares in a VSS scheme. Fourth, we build up a technique to amass the noise share as the QR code.

4. REFERENCES:

[1]. 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.

[2]. 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.

[3]. 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.

[4]. 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.

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

[6]. 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.

[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]. 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.

[9]. C. 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..

[10]. 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..