IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 13, Issue 3, Ver.III (May. - June. 2018), PP 01-06
www.iosrjournals.org

Sharing of a Digital Secret Image by Diverse Media for High Security

Khandelote Pooja Namdev, Prof.V.V.Yerigeri
(Department of Post Graduation, MBES's College of Engineering, Dr Babasaheb Ambedkar Marathwada University, Ambajogai), MS-INDIA
Corresponding author: Pooja Khandelote

Abstract:*-The efficient algorithms require correct protocols for authentication and key management. It is intended to modify the available crypto graphical algorithm to achieve more security and this will be done by incorporating visual cryptography. Conventional Visual Secret Sharing (VSS) schemes are used to hide secret images in the shares that are either encoded or printed on transparencies. Natural Visual Secret Sharing (NVSS) in which various carrier media is used to carry secret images, in which various carrier media is used to carry secret images by a share to protect the secret and the participants during the transmission phase has been proposed. The proposed (n, n) – NVSS scheme shares one digital secret image over (n - 1) arbitrary selected natural images and one noise-like share. Our aim is to use visual cryptography for transmission of the secret image and to protect the network in order to keep the data confidential.*
Keywords- *Visual Cryptography, Natural Visual Secret Sharing, Transmission Risk.*

Date of Submission: 10-06-2018 Date of acceptance: 30-06-2018

I. Introduction

In recent years, information security has become a very important issue due to digitized data can be duplicated and tampered easily. Many methods have received considerable attention for protecting the security of digitized data, such as cryptography, data hiding and secret sharing techniques. Cryptography and data hiding techniques have a common weakness, that is, the security problem of data storage. On the contrary, secret sharing method is a securer one that can enhance the security of digitized data [1-4]. By splitting the digitalized data into several pieces, the risks of data corruption and loss can be decreased [13].

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 [5, 6]. As a result, different security techniques have been used to provide the required protection [7]. 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 [8, 9].

In this paper a method called the natural image based VSS scheme (NVSS scheme) is proposed, which is used to reduce the intercepted risk during the transmission phase [10]. Traditional VSS schemes use a unity carrier for sharing images, which limits the practicality of VSS schemes. But in this method diverse media are used to transmit digital images. This method use digital images, printed images as well as hand-printed pictures. Using diverse media for sharing the secret image would make the hacker's job more difficult. The proposed method can share a digital secret image over n - 1 natural images and one share which is noise share. The natural share contents are not altered in this method, only some features are extracted from each natural share. Thus it greatly reduces the interference probability of these shares. The obtained share that is noise-like can be hidden using data hiding techniques to increase the security during transmission of shares [11, 12].

The proposed method uses diverse media as a carrier; so it has many possible ways to share secret images. For example, suppose a dealer selects n -1 media as natural shares for sharing a secret image. The dealer can choose an image that is not easily recognized as the content of the media, to reduce the transmission risk. To reduce the risk of being suspected, the digital shares can be stored in a participant's digital devices [16]. The printed media can be sent via postal or direct mail marketing services [14]. The transmission risk can be reduced further, since the transmission channels are also diverse. In this paper, an efficient encryption/decryption algorithms for the (n, n) -NVSS scheme is developed. The proposed algorithms can be applied to both digital as well as printed media. A good way for hiding the generated share is also discussed.

The proposed scheme has a high level of user friendliness and manageability; it also reduces transmission risk and increases the security of participants and shares [15].

This paper has the following structure: section II explains about the related works, section III presents the proposed method for sharing secret, section IV presents the result analysis and section V concluded the paper.

II. Related Work

The internet is a general term which provides many services to user. Users can transmit their messages or information to distance friends or go shopping in virtual shops by using the Internet, so it helps us to reduce our precious time. Many types of protection methods are used for preventing the sensitive message to be stolen such as cryptography, visual sharing, and data hiding. The technique that divides a secret image into *n* shares, with each participant holding one or more shares is known as visual cryptography (VC). Any one holding the all n shares when provides those n shares after stacking those n shares will get the relived secret damage which can be recognized by human eyes directly. The secret images can be of various types such as hand written document, printed images, photographs, digital images, others. This technique of sharing & retrieving the images is also known as visual secret sharing scheme (VCC) [1-8].

In 1979 Secret sharing (SS) which were first proposed by Blakley [1] and Shamir [2] independently encode a secret into n shares. This scheme uses polynomial approach to share secret data among n participants. This method assumes that secret is point in K dimension space. SS can not only guarantee the security of information, but also greatly reduce the possibility of secret inaccessible due to misfortune or betrayal, thus it has attracted many scholars' attention. In 1995 (n, n) visual secret sharing (VSS), first proposed by Naor and Shamir [3] is used to encode (encrypt) a secret image into n meaningless share images to be superimposed later to decode (decrypt) the original secret by human visual system after collecting all n secret images. The VSS scheme has a major drawback that is it suffers from high transmission risk because the shares are like noise. As the shares are like noise that causes the attackers attention. Also the meaningless shares are not user friendly &the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares [17]. Then there is new method developed called as ―extended visual secret sharing (EVSS)‖ which uses steganography. Using steganography techniques, secret images can be concealed in cover images that are halftone gray images and true-color images. This EVSS system is more users friendly. But this system to have a drawback that by stego-images still can be detected by steganalysis methods [6-10].

To overcome the drawback of VSS & EVSS scheme the Natural- image based visual secret sharing (NVSS) is proposed. So far, sharing visual secret image via unaltered printed media remains an open problem. In this study, we make an extension of the previous work in [17] to promote its practicability and explore the possibility for adopting the unaltered printed media as shares.

III. Proposed Methodology

An ideal Secret Sharing Scheme must satisfy high security, high accuracy, low computational complexity, and no pixel expansion. All schemes must satisfy the security condition and most of the schemes can reconstruct the secret image accurately. In cryptography, the one-time pad (OTP), which was proven to be impossible to break if used correctly, was developed by Gilbert Vernam in 1917. Each bit or character from the plaintext is encrypted by a modular addition (or a logical XOR operation) with a bit or character from a secret random key of the same length as the plaintext resulting in a ciphertext.

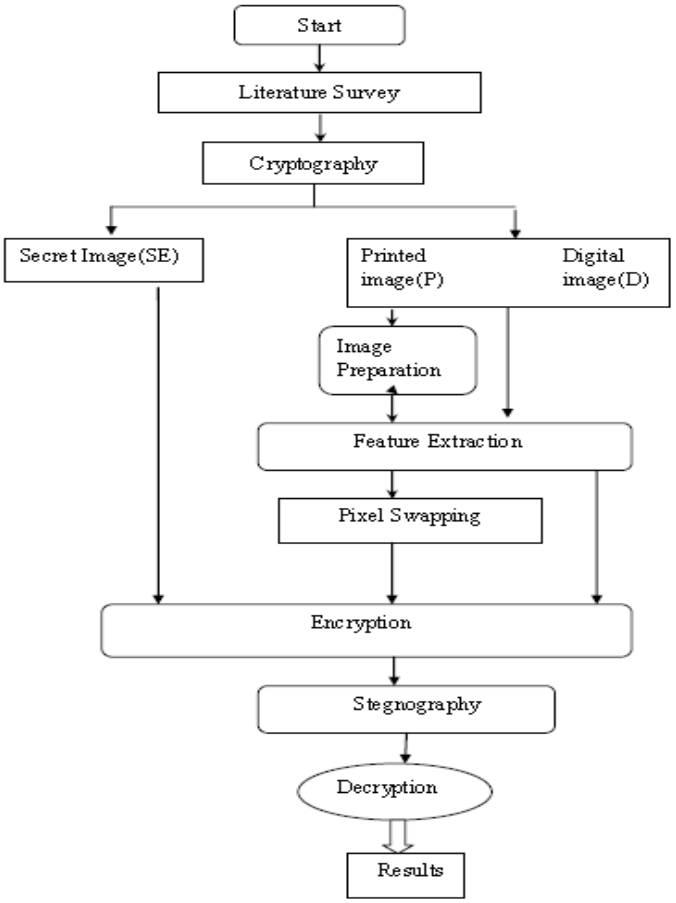


Figure 1: Flow Diagram.

The ciphertext was sent to a receiver; then, the original plaintext can be decrypted in the receiver side by applying the same operation and the same secret key as the sender used for encrypting the ciphertext. As pointed out by Naor and Shamir, the visual secret sharing scheme is similar to the OTP encryption system. In a (2, 2)-VSS scheme, the secret random key and the ciphertext that can be treated as two shares in the scheme were distributed to two participants who involve in the scheme. Instead of generating a secret random key, we extract the secret key from an arbitrarily picked natural image in the (2, 2)-NVSS scheme. The natural image and the generated share (i.e., ciphertext) were distributed to two participants. In decryption process, the secret key will be extracted again from the natural image and then the secret key as well as the generated share can recover the original secret image. The figure 1 shows the flow of the proposed digital image sharing.

A. IMAGE PREPROCESSING

Resize the cropped image with predicted size. The figure 2 shows the preprocessing of image. The image has been cropped to equalize its dimensions with the digital image. In the first step, the content of the printed images is acquired by popular electronic devices. The next step is to cropping the extra images. Finally, the images are resized so they have the same dimensions as the natural shares.

(a) (b)

Figure 2: Cropping of image

B. FEATURE EXTRACTION PROCESS

Feature extraction process is a process that extracts feature images from the natural shares. The module which is the core module of the feature extraction process is applicable to printed and digital images simultaneously.

The three main sub processes in the feature extraction are as follows: binarization, stabilization, and chaos processes. First, binarization process extracts a binary feature matrix is extracted from natural image N. Then the occurrence frequency of values 0 and 1 in the matrix is balanced by the stabilization process. Finally, the chaos process scatters the clustered feature values in the matrix. The figure 3 shows the block diagram of feature extraction.

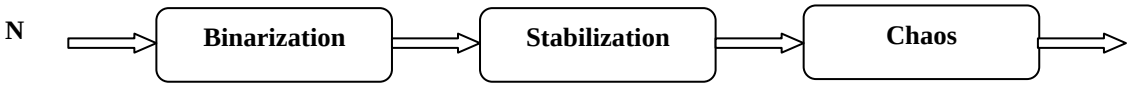


Figure 3: The block diagram of feature extraction [1].

Binarization Process: The binary feature value of a pixel in the feature matrix is decides as follows, by the binarization process.

$$f^{x,y} = F(H^{x,y}) = \begin{cases} 1, & H^{x,y} \geq M \\ 0, & \text{otherwise} \end{cases}$$

$$H^{x,y} = P_R^{x,y} + P_G^{x,y} + P_B^{x,y} \tag{1}$$

M represents the median of all pixel values (Hx1;y1....Hxb;yb) in a block of N.

Stabilization process: The stabilization process balances the number of black and white pixels of an extracted feature image in each block. The number of unbalanced black pixels Qs can be calculated as follows:

$$Q_s = \left(\Sigma_{\forall x1 \leq x \leq xb, \forall y1 \leq y \leq yb} f^{x,y} \right) - \frac{b^2}{2} \tag{2}$$

In the process, there are Qs pixels in which fx;y = 1 is randomly selected and then the value of these pixels is set to 0. The process ensures that the number of black and white pixels in each block is equal.

Chaos process: The feature image extracted and the generated share may contain some texture information, these are eliminated using the chaos process .For this noise is added to the original feature matrix. First, randomly select Qc black feature pixels (fx;y=0) and Qc white feature pixels (fx;y=1) from each block, then alter the value of these pixels. That is, the feature value of a pixel at coordinates (x, y) will be changed to 0 when fx;y=1, and vice versa. Pnoise is the probability to add noise in the matrix, then value of Qc is as follows:

$$Q_c = \frac{b^2}{2} * P_{noise} \tag{3}$$

There may be distortions in the acquired images, which results in noise in the recovered image. When this noise is clustered together the human eyes would be impossible to identify the recovered image. So the pixels-swapping process is used to cope with this problem. This pixel swapping process randomizes the original spatial correlation that may appear in the printed images. The module permutes the feature values of certain coordinates in the feature matrix. After the process, the distortions and the noise is distributed in the recovered image rather than clustered together.

C. ENCRYPTION/HIDNG/DECRYPTION

The encryption and decryption phases are done by setting various parameters as follows:

Encryption: Input includes n -1 natural shares and one secret image. The output is a noise-like share.

Hide the noise-like share: Before hiding the noise like share for further security they obtained share is again encrypted using the RC4 encryption. RC4 is a stream cipher. RC4 generates a pseudorandom stream of bits (a key stream). As with any stream cipher, these can be used for encryption by combining it with the plaintext using bit-wise exclusive-or; decryption is performed the same way. Then this encrypted share is hidden inside another digital image using PVD method. The pixel-value differencing (PVD) scheme uses the difference value between two consecutive pixels in a block to determine how many secret bits should be embedded. This method was found to be more secure than LSB.

Decryption: Input includes n-1 natural shares and one noise-like share. The output is a recovered image. During encryption the feature extraction process is called for each natural image to obtain feature images which are called natural shares. These natural shares are then XOR with the secret image to obtain the share which is called noise like share. During decryption again the feature extraction process is done for each natural image to obtain the natural shares. Then this natural share is XOR with received noise share to obtain the secret image. The figure

4 shows the encryption and decryption process.

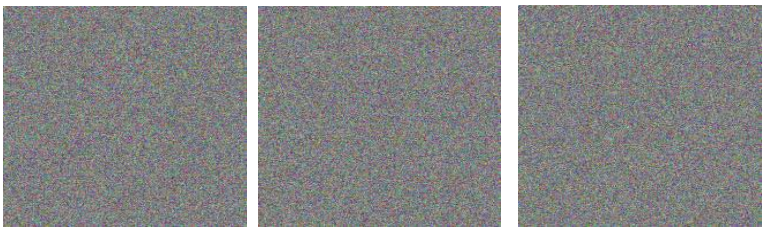
IV. Results And Discussion

This section presents the experimental results of the proposed secret image sharing method. (n, n) secret sharing is applied to demonstrate the feasibility of the method. The test image "Lena" of size 256X256 is selected. The method outlined in this paper is tested by coding the algorithm in MATLAB 17a, a free utility to open, display, modify and save various image file formats, is used for resizing test images. Visual quality of the reconstructed secret image is the factor measured to demonstrate feasibility of 'distortion free' approach.

This section shows the performance of (4, 4) NVSS scheme. The secret image is the well known picture "Lena". Three images are used as digital natural shares as shown in the figure 4 (a, b, c). The generated shares and the recovered image are shown in figure 5 and 6. Figure 5 (a, b, c) shows the generated shares from the natural images and figure 6d shows the share which is noise like and figure 6e is the recovered image.

(a) (b) (c)

Figure 4: Natural Share images.



(a) (b) (c)

Figure 5: The generated shares.

The graphic representation showing the statistical results on the distribution of pixel values in share S and secret image. The distributions of secret in the red, green, and blue color planes are denoted as Secret (R), Secret (G), and Secret (B), respectively. Figure 7 shows that the distribution in Share it is totally different from the distribution in secret. Hence, it is difficult to obtain any information related to secret from share S.

(d) (e)

Figure 6: The noise like share and the recovered image.

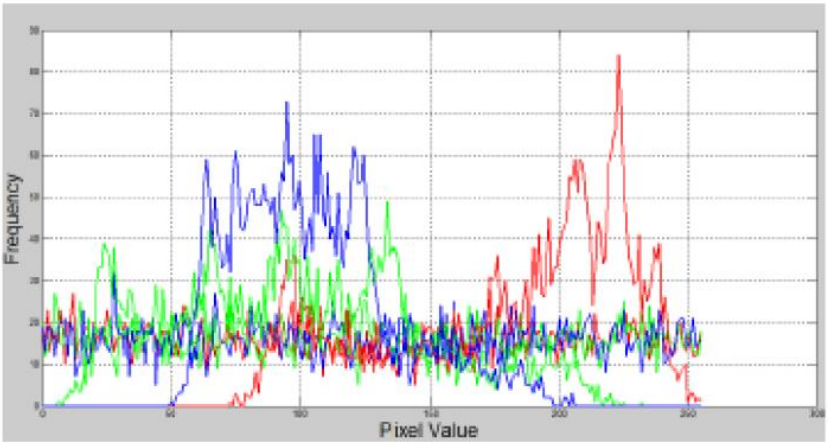


Figure 7: The distribution of the pixel value in share and the secret.

V. Conclusion And Future Scope

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 participant's *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.

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, pp. 1–12, New York, NY, USA: Springer-Verlag, 1995.
[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.
[14]. 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.
[15]. A. Nissar and A. H. Mir, "Classification of steganalysis techniques: Astudy," *Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, Dec. 2010.
[16]. 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. 2013.
[17]. J. Fridrich, M. Goljan, and D. Soukal, "Perturbed quantization steganography with wet paper codes," in *Proc. Workshop Multimedia Sec.*, Magdeburg, Germany, Sep. 2004, pp. 4–15.

Pooja Khandelote. "Sharing of a Digital Secret Image by Diverse Media for High Security." IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) 13.3 (2018): 01-06.