Volume 4, Issue 10, October 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey on Natural Image Based Visual Secret Sharing Scheme (NVSS) in Visual Cryptography

Misha Alexander*
Computer Department & Pune University
Pune, India

Sanjay B. Waykar
Computer Department & Pune University
Pune, India

***Abstract*— Traditional cryptography is a method of transforming message into an unreadable format which is called as cipher text. To read the original data the receiver has to decrypt the message with the secret key.**
Visual Cryptography is a new encryption technique where a secret image is divided into 'n' shares and is transmitted to the participant through various sources. A person who holds 'n' shares can only reveal the secret image. The scheme used for sharing and delivering this secret image is called visual secret sharing scheme , But VSS suffer a lot of transmission risk to solve this problem NVSS(Natural Image based VSS scheme) can be used which can reduce the transmission risk of the secret share.
This paper shows the prospect that image sharing with NVSS is promising.

***Keywords*— Cryptography, Data Hiding, Encryption, Natural VSS, Visual Secret Sharing Scheme.**

I. INTRODUCTION

Rapid growth of Internet which is the collection of computer and communicating devices that are linked together via some wired or wireless media to transmit various range of information and services demands better security. The conventional Cryptography is a method of converting the original data into an unreadable encrypted format called the cipher text. Cryptography makes use of hash function that uses some mathematical function to encode the data which protects the data during transmission it is basically used in ecommerce, military and to transmit confidential data over the communication media. The original data is then decrypted by calculating some hash function [3]. Cryptography ensures confidentiality, data integrity non repudiation, access control and authentication.

Visual cryptography (VC) is a technique that encrypts a secret image into *n* shares, with each participant holding one or more shares. Anyone who holds fewer than *n* shares cannot reveal any information about the secret image [1].When the 'n' shares of the image are put together it reveals the secret image .Visual secret sharing scheme (VSS) is a scheme that is used to share the image securely in a non computer environment [1].The drawback of VSS scheme is that it suffers from transmission risk.

This paper illustrates the NVSS scheme which reduces the transmission risk of the shares.

The remainder of this paper is structured as follows. Section II. Visual Secret Sharing Scheme Section III. Drawbacks of VSS Scheme. Section IV. Natural Image Based VSS Scheme V. Conclusion.

II. VSS SCHEME

In 1994 Moni Naor and Adi Shamir developed the visual cryptography method which is a new way by which the image can be secured; here image is nothing but the plain text. This image is divided into 'n' pieces which are called as shares this process is also called as pixel expansion and it is a part of encryption. These shares are transmitted to the participants. The participants can decode the encrypted image by orderly piling the 'n' shares which will reveal the secret image. Any person without computer knowledge can also decode the cipher text by human vision which will be lucrative for security and defense. The shares are the secret key 'k' that is basically distributed to 'n' participants, the secret can be reconstructed only if the 'k' shares are stacked together [4].

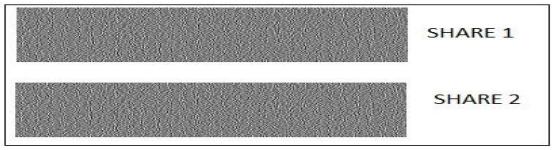

Fig 1: Encryption

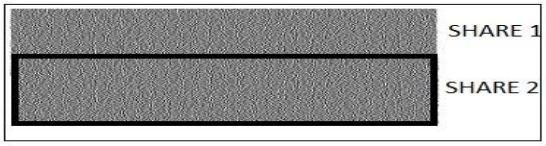

Fig 2:- Stacking of Shares

Fig 3:- Decryption

2.1 (2,2) Threshold Visual Cryptography Scheme

Every pixel of an image is divided into parts. If the pixel is divided into two parts then it has one white and one black block. Every pixel is in proximity to each other.

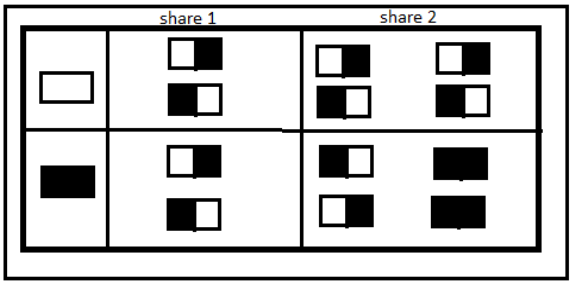

Fig 4:- (2,2) Threshold VCS

2.2 (2,N) Threshold Visual Cryptography Scheme

By considering two nxn matrix S0 and S1 a Visual Secret Sharing scheme is generated as shown below.

S0 = |1 0 0 . . 0| S1 = |1 0 0 . . 0|
|1 0 0 . . 0| |1 0 0 . . 0|

The Boolean matrix S0 has all 1's in the first column and the remaining is all 0's. The matrix s1 is an identity matrix the random permutation is applied on matrix s0 to encrypt the white pixel. In one share there is n-1 white pixel and some black pixel which are placed randomly.

The hamming weight of two black pixels is 2 and hamming weight of two white pixels is one which makes the black pixel darker [4].

2.3 (3, N) Threshold Visual Cryptography Scheme

For n>=3 this scheme will gives 3 out of n scheme. Consider a matrix B which contains 1's only and matrix I which is an identity matrix which contains 1's diagonally and 0's everywhere else. By concatenating matrix B and matrix I we get matrix S1 and matrix S0 is the complement of matrix S1 [4].

2.4 (K,K) Threshold Visual Cryptography Scheme.

The k out of k scheme describes pixel expansion of 2k-1. Two matrix are constructed S0 which contains even number of 1's and all Boolean 'n' vectors while S1 matrix which contains odd number of 1's and Boolean vectors elsewhere.

2.5 (K,N) Threshold Visual Cryptography Scheme

Consider a matrix IM whose column is equal to set of vectors. Matrix IM is an nxl matrix which contains elements such as A= {a1,a2…….an)[4].

III. DRAWBACKS OF VISUAL SECRET SHARING SCHEME

The technique which is used to transmit or deliver the secret image over the network is known as visual secret sharing scheme (VSS) [1].The major drawback of (VSS) scheme is that it suffers from high transmission risk as the shares are like noise which causes the attackers attention and the shares can be intercepted [1].The VSS scheme is not user friendly [1].The VSS limits its practicality by using unity carrier for sharing the images.

IV. NATURAL IMAGE BASED VSS SCHEME

Natural Image Based Visual Secret Sharing Scheme (NVSS) is a method that is introduced to reduce the transmission risk that occurs in the VSS Scheme [1]. The NVSS makes use of natural image such as photographs, paintings, landscapes etc as digital shares, making use of natural shares rather than noise like image can reduce the transmission risk to certain extent [1]. The NVSS scheme also makes use of different media to transmit the share this will make the catch of data difficult.

The NVSS scheme uses the one time pad (OTP) technique .OTP is a java program that encrypts the image, after encryption the image contains only black and white pixels and it is very difficult to extract the information making it un intercept able .In (2, 2) VSS Scheme we make use of random generated key and the cipher text as the two shares, these two shares are distributed to the participants. In NVSS scheme the secret key is extracted from the randomly selected natural image. In the process of encryption the natural image and the generated secret key is sent to the participants. During the decryption secret image

In the process of encryption the natural image and the generated secret key is sent to the participants. During the decryption secret image and the generated image reveal the original image. The NVSS can also be extended to (n, n) NVSS scheme.

4.1 Encryption Process in NVSS (n, n) scheme

The encryption process in NVSS consists of two phases the feature extraction phase and the encryption phase.

4.1.1 Feature Extraction Process

In feature extraction process some features are extracted from the natural shares i.e. both the printed image and the natural image simultaneously using wave transform method. Wavelet transform method is a mathematical method for compressing the image and for processing the digital signals [6]. The extracted feature is an image that looks somewhat like the original image this extraction reduces the randomness and hence the security of the share.

The feature extraction has three processes binarization, Stabilization and Chaos. From the natural image N the feature matrix is extracted after extracting the feature matrix the other three processes are applied to it.

A simple threshold function F is used to determine the binary feature value of a pixel this process is called binarization. The extracted feature of each block in binarization process is balanced using the stabilization process i.e. the black and white pixels of each block are balanced .

After stabilization the chaos process is applied this process which adds noise in the matrix which can disorder the original matrix that will not reveal the texture of the image from the original share.

4.1.2. Image Preprocessing

In this process the printed image that is captured or acquired by digital cameras or smart phones are cropped so that the extra image is removed and then the acquired image is resized so that its dimensions matches the natural shares . Printed images are needed to transmit the secret image.

4.1.3. Pixel Swapping Post processing

Pixel swapping is done in order to add randomness to the image. Two pixels are picked from random column and swapped if upper pixel has higher hue. The pixels of the random row are selected and swapped so the left pixel will have higher brightness than the right. This process is repeated on the complete image [7].

4.2 Encryption / Decryption Process

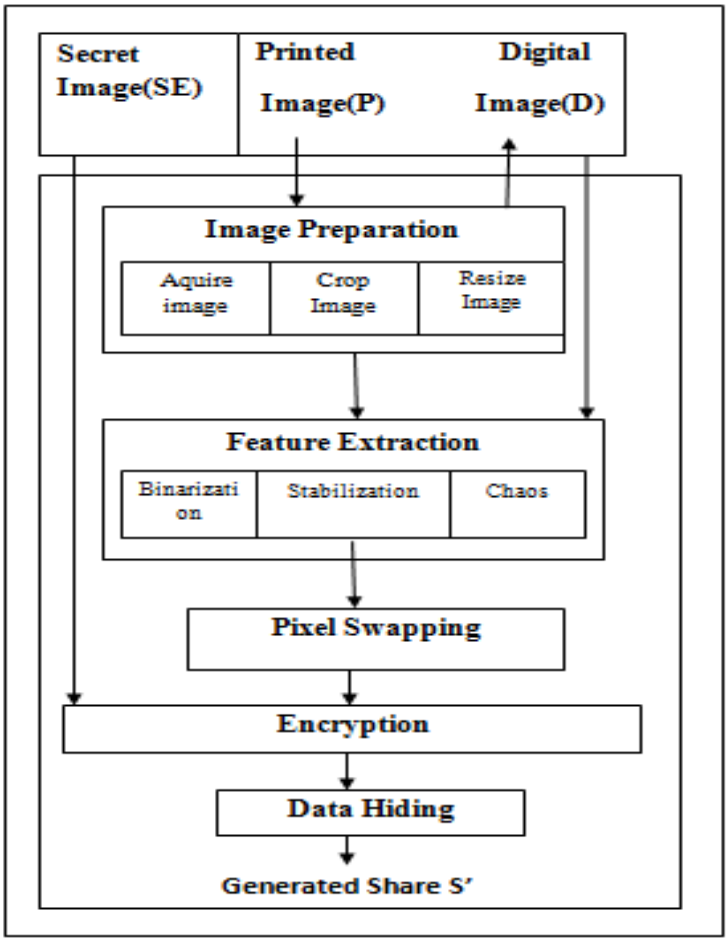

Fig 5:- Encryption Process

The input of Encryption process is a secret image and the n-1 natural shares and the output of the Encryption process is a noise like image. The binary feature of the natural share is extracted and the XOR operation of secret pixel and binary feature value is performed. This process randomly distributes the pixel values in the feature image [1]. The generated share after the encryption process is secure as this encryption process has the following properties and hence it is impossible to crack it [1].

Property 1:- The amount of information required for the generated share is the same as for the secret image [1].
Property 2:- Pixel values in a feature image are distributed uniformly over [0, 255] [1].
Property 3: - Pixel values in a feature image are distributed randomly [1].
Property 4:- The generated share is secure [1].

4.3 Data Hiding

To further reduce the transmission risk the data hiding techniques such as Steganography and Quick Response Code (QR code) is used to hide the noise like share during the transmission. Steganography is a technique to hide information inside information which will secure the secrecy of transmission [9].

A QR ("quick response") code is a two dimensional barcode Invented by the Japanese corporation Denso Wave. Information is encoded in both the vertical and horizontal direction, thus holding up to several hundred times more data than a traditional bar code [8]. QR code is used as a carrier for secret communication.

4.4 Decryption Process

In the decryption process from the stego-share the share is extracted. The feature matrix F is extracted from the numeric string SQR then decoded which is in the QR code format [1].

V. CONCLUSION

It can be concluded from the above survey that the NVSS scheme effectively reduces the transmission risk by using natural image as shares and data hiding techniques such as stenography and QR Code. NVSS scheme is also a user friendly technique for the participants and shares.

REFERENCES

[1] Kai-Hui Lee , Pei-Ling Chiu, "Digital Image Sharing by Diverse Image media",IEEE Transactions on Information Forensics and Security, vol 9, No. 1,pp.88-98,January 2014.
[2] Sagar Kumar Nerella, Kamalendra Varma Gadi, RajaSekhar Chaganti " Securing Images Using Colour Visual Cryptography and Wavelets ", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 2, Issue 3,pp.162-168, March 2012.
[3] Prakash Chandra Jena1, Nikunja Kanta Das, "Survey Paper: Cryptography Is The Science Of Information Security", International Journal of Emerging Technology and Advanced Engineering,vol 3, Issue 8,pp.227-236 August 2013.
[4] Maneesh Kumar , Sourav Mukhopadhyay "Visual Cryptography for Black and White Images", International Journal of Information and Computation Technology. Vol 3,pp. 1149-1154,November 11 2013
[5] http://www.r-hansen.com/tech/oti.html
[6] http://whatis.techtarget.com/definition/wavelet
[7] http://blog.hvidtfeldts.net/index.php/category/pixel-reshuffling/
[8] Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Lindsay Munroe, Sebastian Schrittwieser, Mayank Sinha, Edgar Weippl" QR Code Security" SBA Research Favoritenstrasse 16 AT-1040 Vienna,Austria.
[9] T. Morkel , J.H.P. Eloff , M.S. Olivier" An Overview Of Image Steganography", *Proceedings Of TheFifth Annual Information Security South Africa Conference*, June/July 2005.
[10] M. Naor And A. Shamir, "Visual Cryptography," In *Advances In Cryptology*, Vol. 950. New York, Ny, Usa: Springer-Verlag, 1995, Pp. 1–12.
[11] 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.
[12] 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.

