

Literature Survey on a NVSS Scheme for Sharing Digital Secret Image

Nasla K

Computer Science and Engineering, University of Calicut/ KMCT College of Engineering Calicut, India

Abstract: Usual visual secret sharing scheme hide secret images in shares they are either printed or in digital form. Meaningful images or noise like pixels are appear due to hiding secret image in shares, but during the transmission of share it will increase interception risk. So visual secret sharing scheme suffer from transmission risk problem. To solve this problem the author proposed a natural image based visual secret sharing scheme. In that secret images are transferred through various media to secure the secret and participant. The proposed scheme can share one digital secret image over $n-1$ arbitrary selected natural images and one noise-like share. Natural image is a combination of printed and digital image. Natural image and printed image generate one noise like share. The unaltered natural shares are different, thus reducing the transmission risk problem

Keywords: visual secret sharing scheme, natural image based visual secret sharing scheme, conventional VSS scheme, natural images, transmission risk.

1. Introduction

Recent advancement in Internet technology has enabled information sharing and has brought the world closer. At the same time security concern has grown proportionally. This makes organizations, institutions and spending excessive amounts of money to secure their data. Instead of the security of sharing secret information, people usually conceal the secret data with symmetric or asymmetric cryptography, these cryptographic methods should require high computation cost in encryption and decryption processes. Therefore, many visual cryptography schemes were proposed. Visual cryptography is an efficient secure method for hiding a secret image by dividing it into shares and any one can decode it easily by the human visual system. The main concept of the original visual cryptography scheme is to encrypt a secret image into n meaningless share images. It does not leak any information of the shared secret by any combination of the n share images except for all of images. Having the ability to hide information such as personal details is very desirable.

When the data is hidden within separate images, it is completely unrecognizable. While the shares are separate, the data is completely unintelligible.

Each image holds different pieces of the data and when they are brought together, the secret can be recovered easily. They each rely on one another in order to obtain the decrypted information. There should be no way that anyone could decipher the information contained within any of the shares. When the shares are brought together, enciphering is possible when the shares are placed over one another. At this point, the information becomes instantly available. No computational power is required at all in order to decrypt the information. All decryption is performed by the human visual system (HVS). This kind of problem is formally referred to as a secret sharing problem.

2. Proposed Scheme

Natural image based visual secret sharing scheme [1] is having a three process. The [1] feature extraction algorithm consist of three steps a) Binarization b) Stabilization c) chaos. In binarization process image is converted into 0's and 1's. Stabilization is used for searching black and white pixel from image. In last chaos introduce noise. In encryption algorithm with the help of secret image and feature extracted from natural image combine to form noise like share and at last generate the quick response code. QR code is used to store amount of data.

3. Literature Survey

Visual cryptography needs only the characteristics of human vision to decipher the encoded images. It does not need any cryptographic knowledge or any kind of complex computation to decipher the encoded image. Mainly this visual cryptography focuses on the security aspects to uphold the secret image from two or more cover images so that any attacker cannot retrieve any data. Naor and Shamir proposed the basic model of the visual cryptography, starting from their many visual cryptographic methods evolving day by day. Hence to uphold good confidentiality in transmitting of secret data via images in internet, selection of good visual secret sharing scheme is necessary. Therefore it is necessary to study all the recent technologies that are evolved and written as a literature to understand the concept of visual cryptography in a better way.

Hence to promote good confidentiality in transmitting of secret data via images in internet, selection of good visual secret sharing scheme is necessary. Therefore it is necessary to study all the recent technologies that are evolved and written as a literature to understand the concept of visual cryptography in a better way Most secret sharing schemes are based on cryptography such that the encryption and decryption processes need high computation costs. Visual secret sharing schemes hide the secret image into several share images and

distribute these share images to participants. With no computation, human beings are able to obtain the secret image by stacking the share images.

Naor and Shamir's initial implementation [2] believes that the image or message is a collection of black and white pixels, each pixel should be handled individually and it should be noted that the white pixel represents the transparent color. One shortcoming of this is that the decryption process is lossy, the area that suffers due to this is the contrast. Contrast is very important within visual cryptography because it determines the clarity of the recovered secret by the human visual system.

Ran-ZanWang and Yung-Ching Lan proposes an incrementing VC scheme [3] using random grids. The method has the same incremental revealing effect to the secrets on an image, and the size of each share is the same as that of the original image without any expansion. The smaller size of shares makes their further processing such as storage and/or printing out more efficient.

Kai-Hui Lee and Pei-Ling Chiu[4] proposed Extended visual cryptography scheme consider n-number of natural image and one secret image. Extended visual cryptography scheme generate a noise like shares with every share associate a cover image and in that cover image hides a secret image. The algorithm which has been proposed in this method is easy to maintain for both sender and receiver because they know that in which cover image is hidden. It is easy for receiver also to combine cover image and extract secret image. In this paper they propose general approach to clarify the pixel expansion problems, this approach only for binary secret images. There are two phases in this proposed approach. First phase based on a given access structure, in this phase using an optimization technique they construct meaningless shares. In second phase using stamping algorithm they add cover image in each shares. The experimental result display that problem of pixel expansion is solved by extended visual cryptography scheme for general access structure. In this paper cover images are added with each share so it tampers the security.

Tzung-Her Chen and Kai-Hsiang Tsao[5] proposed that a visual secret sharing technique based on random grid visual secret sharing algorithm this method is announced by Kafri and Keren in 1987. In this secret image and natural image pixel is divided into two grades grade1 and grade2 depending on which pixel is move on which grade. And at the receiving end grade1 and grade2 is combined, then move the pixel in grade1 and grade2 depending on which pixel belong to which grade. In this paper they propose random grid visual secret sharing, does not introduce any pixel expansion. To achieve two meaningless random grids G1 and G2, the first random grid G1 is achieved by selecting the color white or black. Then, given a certain private pixel and the grid pixel of G1 and grid pixel of G2 is resolved. G1 and G2 stacked results are always fully black although the private is black and white or black with $\frac{1}{2}$ probabilities although the private is white. In this way the private is recognizable through stacked random grid. In this paper at the receiving end receiver cannot get the image properly because when they move pixel in grade 1 and grade 2 that time image pixel value is mismatch. It also affects the brightness of original image.

Cheng Guo and Chin-Chen Chang propose a system of secret image sharing in groups [6] with multi-threshold access structure. In such a case, multiple secret images can be shared among a group of participants, and each secret image is associated with a (potentially different) access structure.

4. Conclusion

The paper propose visual secret sharing scheme Natural image based visual secret sharing scheme hide secret image over n-1 arbitrary selected natural shares. Therefore they are totally secure. Therefore visual secret sharing scheme reduce the transmission risk problem and provide security for secret image. With the help encryption algorithm extended visual cryptography scheme for general access structure reduces the pixel expansion problem. The major contribution of our work is, it reduces the pixel expansion problem. Major contributions are this is the first attempt to send secret image through various carrier media and for image sharing hand printed image is successfully introduced and third one is to generate quick response code to store noise shares.

References

- [1] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media" IEEE Transactions Vol. 9, No. 1, January 2014.
- [2] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12
- [3] 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.
- [4] Kai-Hui Lee and Pei-Ling Chiu, "An Extended Visual Cryptography Algorithm for General Access Structures," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, February 2012
- [5] 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.

Author Profile



Nasla k received the B. Tech degree in Computer Science and Engineering from the University of Calicut, Kerala, India, in 2013, and pursuing her M. Tech degree in Computer Science and Engineering in the same University. Her research interests include image processing, software engineering.