International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 08 | August -2020 ISSN: 2582-3930

Secure and lossless (k, n) secret image sharing schemes: a review

Shubham B. Bhokare[1], Archana S. Vaidya[2]

[1]*Computer Engineering, Gokhale Education Society's R. H. Sapat College of Engineering Management Studies and Research, Nashik-5, Maharashtra, India*
[2]*Computer Engineering, Gokhale Education Society's R. H. Sapat College of Engineering Management Studies and Research, Nashik-5, Maharashtra, India*

Abstract - The majority of generated information includes images as they are widely used in the industrial process, businesses, military, scientific and researches. Information security has become a serious issue as a huge amount of information is exchanged via the internet. It needs to protect the confidential data in the image from unauthorized access or intruders. Advancement in hacking techniques has failed traditional image encryption approaches. Image encryption is applied to increase its security when used over the internet and to protect an image from unauthorized access. Nowadays the Internet is being used by everyone for sharing, transferring and storing huge amounts of data. The Internet has many drawbacks and there exist possibilities of hacking or being attacked by intruders. The main objective of this is to review the work carried out to secure secret image sharing using different approaches. We concern that our present, specifically in epitomizing the earlier discovery and in analysing the directions for future research in this area.

Key Words: Image Encryption, Secret Image Sharing, Sharing Matrix, Visual Cryptography.

1.INTRODUCTION

The information generated from devices over rapidly growing internet needs to be secured. Most often cryptography is used to secure information. Original readable information is encrypted and converted into ciphertext and then decrypted to retrieve original information in a readable format. With rapid development in technology, intruders or hackers can find a way to access or modify confidential data. So, this information, when shared over a network, must be protected by applying security techniques like cryptography. Cryptography provides Authentication, Confidentiality, and Integrity to the information when shared.

This article gives an overview of various secret images sharing schemes, also analyses the performance of them based on different performance measures. This article is laid out as follows: Section 2 gives an analysis of the concept of Visual Cryptography (VC), Polynomial Based Secret Image Sharing (PSIS), Visual Secret Sharing (VSS), Halftone Visual Cryptography, Secret Sharing using Meaningful images, Threshold Based Secret Image Sharing (TSISS). Section 3 gives a performance analysis of different SIS schemes on the basis of various parameters. Finally, Section 4 concludes by summing up the different Secret Image Sharing Schemes.

2. Secret Image Sharing Techniques

2.1 Visual Cryptography (VC)

Secret image sharing has attracted significant consideration in recent years. At first, Visual Cryptography methods were proposed by Naor et al. [1] The secret image in VC is encrypted into n shares/shadows. These n shares are allocated to each participant. They can have either one or more shares. All the participants in the system have to combine n shares in (n, n) VC scheme to regenerate the original image. The Encryption process hides visual data and the decryption is performed by human vision. Encryption process inserts some noise data in the original image so as to hide the information and while decryption, the noise data is reduced or removed to regenerate original information.

In VC,

- Every share is transparent, independent and noise-like.
- It supports only binary images.
- Attackers can identify and modify image shares as they are noisy in nature.
- Reconstructed image is always of low quality.
- Large transmission and storage costs is required.

2.2 Polynomial Based Secret Image Sharing (PSIS)

Shamir et. al. [2] proposed Polynomial-based Secret Image Sharing (PSIS). Lagrange interpolation was used to generate shares of the secret image and retrieve original with minimum number of shares.
However,

- It requires a huge computations cost in the regeneration phase.
- Successful regeneration depends on number of shares and the sequence in which they appear and
- The results are in a different data range from one of original image

2.3 Visual Secret Sharing (VSS)

Yang et al. [3] has also suggested novel (k, n) probabilistic visual secret sharing (VSS) schemes with non-

expandable sizes of shares. They have presented various (k, n) schemes depending on the probability technique. The contrast level of this method is the same as the conventional VSS schemes. They have also demonstrated that the conventional VSS scheme can be changed to a probabilistic VSS scheme by using the transfer function.

2.4 Halftone Visual Secret Sharing(H-VSS)

Alex et al. [4] used various methods for error diffusion to improve quality of the image in the halftone shares of the secret image to be shared. They have used halftoning in which the continuous-tone image is transformed into a binary image by applying visual secret sharing (VSS) and then use visual cryptography (VC). The halftoning of images is used to add secret information pixels into not coded halftone shares. The secret image is converted into a halftone image by gaining visual information. It gets this significant visual information by applying error diffusion to halftone shares simultaneously. The regenerated image is obtained by gathering qualified shares together. Cross-interference of shared secret images does not hamper anything.

2.5 Secret Sharing with Meaningful Images

Tso et al. [5] introduced a novel image sharing method to satisfy numerous problems such as

- Pixel Expansion problem.
- Low quality of reconstructed image and creating useless shares for image sharing.

This method firstly decomposes the secret image to be shared then encodes them into n number of shares. These image shares are then implanted into cover images. This approach is useful for constructing the meaningful shares of the images to be shared. The size of both the original secret image and the generated share is the same. On the receiver side when all the shares are combined to form a stack the quality of the reconstructed image is better and it has no distortion.

2.6 Threshold Based Secret Image Sharing (TSISS)

Teng Guo et al. [6] introduced (k, n) - TSISS - a (k, n) threshold based secret image sharing scheme. It breaks a secret image to be shared into n number of shares such as any k number of shares can be combined to regenerate the original secret image, but no less than k shared shadows can provide any information about the secret image. They have added an AES encryption process previous to the sharing process to generate a computationally secure (k, n) - TSISS. It combines the advantages of small share size with the guarantee of computational security.

2.7 Halftone Visual Cryptography

Z. Wang et al. [7] have introduced Halftone Visual Cryptography (HVC) via error diffusion, which generates the shadows of pleasing visual information. They have used Error diffusion to construct the shadows such that the noise brought by the current pixels is diffused away while generating the halftone shadows. The secret image data is then naturally embedded into the halftone shadows. The isotropic and homogeneous distribution of the current pixels imposes the minimal noise in error diffusion, leading to shares with very good image quality. It follows the basic principle of visual cryptography, guaranteeing the security of the construction scheme. A large quality index leads to visually pleasing halftone shadows, but it also brings higher contrast loss in the regenerated images. This method gives visually pleasing halftone shadows.

3. Comparison

Table below shows comparison of various Secret image sharing techniques –

Schemes	Pixel Expansion	Data Loss	Reconstruction Cost	Original Image
VC	Yes	Large	No	Binary
PSIS	Yes	Small	Large	All
Halftone	Yes	No	Small	Binary
SISSM	Negligible	No	Small	All

4. CONCLUSIONS

In this paper a glimpse with the insight of the various secret image sharing techniques, their outcomes with respect to performance measures and their disadvantages are enumerated with respect to securing data are discussed. This paper also spotlights the existing work limitations and its merits. Pointing out open issues and techniques to be carried out leads us to come out with better performance measures in real time directs for Future Research.

ACKNOWLEDGEMENT

I Would like to thank Department of Computer Engineering, G. E. Society's R. H. Sapat College of Engineering and Management Research.

REFERENCES

1. Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in CryptologyEUROCRYPT'94. Springer Berlin/Heidelberg, 1995.
2. Shamir, How to share a secret, Communication of ACM, vol. 22, no. 11, pp. 612613, Nov. 1979.
3. Yang, Ching-Nung. "New visual secret sharing schemes using probabilistic method." Pattern Recognition Letters 25.4 (2004): 481-494.
4. Alex, Nitty Sarah, and L. Jani Anbarasi. "Enhanced image secret sharing via error diffusion in halftone visual cryptography." Electronics Computer Technology (ICECT), 2011 3rd International Conference on. Vol. 2. IEEE, 2011
5. Tso, Hao-Kuan. "Secret Sharing Using Meaningful Images." Journal of Advanced Management Science 1.1 (2013)
6. Teng Guo, Feng Liu, ChuanKun Wu, ChingNung Yang, Wen Wang, and YaWei Ren. Threshold Secret Image Sharing. Information and communication security v 8233 Nov 2013

7. Z. Wang, G. Arce, and G. Di Crescenzo, Halftone visual cryptography via error diffusion, IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 383396, Sept 2009.
8. Longdan tan, yuliang lu, Weighted Secret Image Sharing for a(k,n) Threshold Based on the Chinese Remainder Theorem. vol. 7, Sept 2019
9. Dong Xie, Lixiang Li1, A Secure and Efficient Scalable Secret Image Sharing Scheme with Flexible Shadow Sizes January, 2017
10. Sagar Nitharwal, A Boolean-based multi-secret image sharing scheme using bit-reversal, Dec 2017