A Framework for More Secured and Authenticated Image Sharing Schemes

Miss. S. V. Kale Dr. V. M. Thakare Dr. Mrs. S. S. Sherekar

Abstract- **Image secret sharing schemes have been research area of image transformation with lots of secret schemes. This paper focuses on different schemes, such as Extended Visual Cryptographic Schemes (EVCS), Visual Secret Sharing Schemes for plural secret images (VSS-q-PI), Threshold Multiple-Secret visual cryptographic schemes (MVCS), Secret image sharing procedure, Secret image retrieving procedure, The Two-Phase Encryption Procedure . But some problems exists in each method, So as to overcome the problems that are given in analysis and discussion, The improved "visual secret sharing with encryption decryption schemes" sharing method for secure transformation is proposed using the analysis of the various mobility models.**

Keywords- **Image encryption, Image secret sharing, Secret sharing, Secret sharing schemes, Visual secret sharing schemes.**

I. INTRODUCTION

Secret sharing is an important technique that can be used to protect the confidentiality of information. Concept of visual

secret sharing (VSS) according to the mechanism, a secret image is embedded into the cover image to generate k shadow

images [1]. Visual cryptography schemes (VCSs) generate random and meaningless shares to share and protect secret images. The secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret [2]. The aim of this paper is to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images [3]. This paper, discusses different secret image sharing schemes such as Extended Visual Cryptographic Schemes (EVCS), Visual Secret Sharing Schemes for plural secret images (VSS-q-PI), Threshold Multiple-secret Visual cryptographic schemes (MVCS), Secret image sharing procedure, Secret image retrieving procedure[1], The Two- Phase Encryption Procedure. These secret image sharing schemes provide the more secured transmission, formulation and constructions of VSS schemes realizing a general access structure for multiple secrets without any restrictions. But these methods also have some problems. To overcome such problems improved version of sharing scheme that is "visual secret sharing with encryption decryption schemes" sharing method for secure transformation is proposed using the analysis of the various mobility models.

II. LITERATURE SURVEY

Many studies on sharing models have been done to developthe more secured sharing scheme in recent past years. Such schemes are:A simple (2, 2) secret image sharing scheme that can simultaneously extract the original secret image and reconstruct the original cover image without distortion [1]. A binocular VCS (BVCS), called the (2, n)-BVCS, and an encryption algorithm are proposed to hide the shared pixels in the single image random dot stereograms (SIRDSs) [2]. Secret Sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret [3]. This paper introduces sharing scheme i.e. Extended Visual Cryptographic Schemes (EVCS), Visual Secret Sharing Schemes for plural secret images (VSS-q-PI), Threshold Multiple-secret Visual Cryptographic Schemes (MVCS), Secret image sharing procedure, Secret image retrieving procedure, The Two-Phase Encryption Procedure. The paper is organized as follows: **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobility models. **Section VI** proposed methodology. **Section VII** outcome of results. Finally **Section VIII** Conclusion.

.

III. PREVIOUS WORK DONE

In research literature, many sharing models have been studied to provide various secret sharing schemes and improve the performance in terms of more secured transmission, formulation and constructions of VSS schemes realizing a

general access structure for multiple secrets without any restrictions. Ching-Chun Chang et al., (2016) [1] have worked on Protecting the confidentiality of information. Secret sharing is an important technique that can be used to protect the confidentiality of information. Kai-Hui Lee et al., (2014) [2] has proposed the Visual cryptography schemes (VCSs) generate random and meaningless shares to share and protect secret images. Pei-Ling Chiu et al., (2014) [3] has proposed a *(2, 2)*-VCS using the halftoning technique to construct meaningful binary images as shares carrying significant visual information. sharing secret images via highquality shares. The visual quality of the halftone is significantly better than that attained by extended VC. Manami Sasaki et al., (2018) [4] has presented the analysis of various schemes with the secret sharing (SS) scheme. This scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret. Yodai Watanabe et al., (2015) [5] have shown the impact of to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images. This scheme uses SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. The encryption algorithm alters the random dots in the SIRDSs according tothe construction rule of the *(2, n)*-BVCS to produce nonpixel expansion shares of the BVCS.

IV. EXISTING METHODOLOGIES

Many sharing schemes have been implemented over the last several decades. There are different methodologies that are implemented for different secret sharing models i.e Extended visual cryptographic schemes (EVCS), Visual Secret Sharing Schemes for Plural Secret Images (VSS-q-PI), Threshold Multiple-secret Visual Cryptographic Schemes (MVCS), Secret Image Sharing Procedure, Secret Image Retrieving Procedure, The Two-Phase Encryption Procedure.

4. 1 SECRET IMAGE SHARING PROCEDURE SECRET IMAGE RETRIEVING PROCEDURE

This scheme proposes a simple (2, 2) secret image sharing scheme that can simultaneously extract the original secret image and reconstruct the original cover image without distortion. One distinguishing feature of proposed scheme is that it is adaptive, i.e. the payload can be changed easily according to the control parameter ω. Moreover, trade-offs between the payload and the quality of the shadow images can be achieved by adjusting ω to appropriate values. Overflow and underflow problems also can be handled easily. In addition, proposed scheme is computationally efficient, since no time-consuming mathematical operations are involved [1].

4. 2 TWO-PHASE ENCRYPTION PROCEDURE

It is a mathematical optimization model to find an optimum solution to share a secret image in SIRDSs where the objective is to maximize contrast under the constraint of the visual quality of SIRDSs. Using this model, dealers can adjust the visual quality of SIRDSs to obtain the best display quality of the recovered images. The pixel distribution among shared pixels must obey the construction rules or codebooks of the VCS. Shared pixels mean that a set of pixels shares the same secret pixel in a VCS. The Two-Phase Encryption Procedure propose a *(2, n)*-BVCS for sharing a binary secret image in *n* SIRDSs. The encryptor alters pixels only within a specific region, which is called the encryption region, where black secret pixels appear. Various sharing models have been proposed with their analysis and impact of performance in image transmission [2].

4. 3 EXTENDED VISUAL CRYPTOGRAPHIC SCHEMES (EVCS)

Extended Visual Cryptography Scheme is a user friendly scheme, in which the share contains many noise-like pixel or display low-quality images. This type of share can be easily detected by the naked eye so it can be tracked by the attackers. Extended visual cryptographic schemes EVCS assumes an access structure such that all but one of its qualified sets consist of (the combination of) a single share, **VSS-q-PI** an access structure whose forbidden sets are identical for all secrets3 (although its qualified sets can be arbitrary) and **MVCS** a threshold access structure. This work provides the formulation and constructions of VSS schemes realizing a general access structure for multiple secrets without any restrictions. [3].

4. 4 VISUAL SECRET SHARING SCHEMES

A secret image is encrypted into two shares. Each share is indistinguishable from noise images, and so leaks no information about the secret. On the other hand, the secret image can be reconstructed when both of the shares are superposed. This can be constructed as follows. A pixel e in the secret image is encrypted into two subpixels in each of the two shares. In this proposed scheme, scheme is a (2, 2) secret image sharing scheme, which should guarantee that none of the shadow images can leak any useful information about the secret image [4].

V. ANALYSIS AND DISCUSSION

VSS schemes encrypting multiple images allow the authentication. A simple (2, 2) secret image sharing scheme that can simultaneously extract the original secret image and reconstruct the original cover image without distortion [1]. A binocular VCS (BVCS), called the (2,n)-BVCS, and an encryption algorithm are proposed to hide the shared pixels in the single image random dot stereograms (SIRDSs) [2]. Secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret [3].Visual cryptography schemes (VCSs) uses halftoning technique to construct meaningful binary images as shares carrying significant visual information. sharing secret images via high quality shares. The visual quality of the halftone is significantly better than that attained by extended VC[4].

Mobility scheme	**Advantages**	**Disadvantages**
Extended visual cryptographic schemes (EVCS)	This method can deal with greyscale input images, has smaller pixel expansion, always unconditionally secure, does not require complementary share images, one participant only needs to carry one share and can be applied for general access structure.	Different protocols used by EMOR have different drawback. AODV has high packet loss CBF suffer from high latency. GPSR does not give better delivery ratio. OR suffer from duplicate packet due to failure of coordination zone and also more than on node send same packet if they can not overhear each other.
Visual Secret Sharing Schemes	Simple to implement. Lower computational cost. authentication can be done using shares to prevent the systems from some attacks.	The contrast of the reconstructed image is not maintained. Due to pixel expansion the width of the decoded image is twice as that of the original image. Leads to loss of information due to change in aspect ratio. Additional processing is required for colored images.
Secret Image Sharing Procedure	This proposed method is very efficient and scalable, High security, High efficiency, Noiseresilient capability, Flexibility.	The drawback of this method cannot predict the interference beyond the Gaussian. Due to more complex and dynamic nature of method it takes more time.
Secret Image Retrieving Procedure	The advantages of this method are its simplicity, high imperceptibility and high capacity.	This method is a very fragile method and does not tolerate any manipulation. Even slightest modification to the image or change of format destroys the hidden data.
Two-Phase Encryption Procedure	This method provides high security against unauthorised alteration. Message secrecy and Robustness is high.	This method is very time consuming. Difficult to implement.

Table-1: Comparisons between different secret-sharing Schemes

VI. PROPOSED METHODOLOGY

Secret image sharing scheme is important and difficult task to analyse and discuss about various methods based on different

parameters i.e accuracy, transmission, time, throughput, delay, capacity, pixel value etc for different sharing models. There are still problems which trouble in this field. New sharing method called "secret image sharing with encryption decryption" model for secret sharing model is propose here to overcome the problems of this model. This section describes the feature extraction module that extract feature images from the natural shares. The proposed system consists of a original

image- based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. For this process the share contain arbitrary number of original natural images and one noise like share. Visual cryptography is a method used to encrypt a secret image into n shares (share1, share2,..) in which every participant holding one or more shares. The proposed (n, n)-NVSS scheme can encipher a truecolor secret image by n- 1 natural shares and one noise like share. Before encryption (resp. decrypt) of each bit-plane of the secret image, the encryption algorithm first extracts n-1 feature matrices from n - 1 natural shares. Then the bit-plane of the reconstruct (secret image) feature matrices execute the XOR operation. Therefore, to encrypt (resp. decrypt) a true-color reconstruct (secret image), the encryption (resp. decryption) procedure must be performed iteratively on the 24 number of bit-planes. The input natural shares (N1,…..,Nn+1_)of the scheme include np printed images and nd digital images (np > 0, nd > 0, and n =np +nd + 1). The np printed images must be processed and transformed into digital form in the image preparation process.

Encryption:

Step 1: Preprocessing - Convert an image into halftone. Halftone process, in printing images, a technique of breaking up an image into a series of dots so as to reproduce the full tone range of a photograph or tone art work. In this program, the input gray image will be converted into halftone image of same size using Floyd's Error Diffusion Method.

Step 2: share 1 and share 2 images With left and right component of image

Step 3: combine preprocessed image+ share1+share2

Step 4: encryption algo.

Decryption:

Step 1: Decryption using key RSA algo. (Put your logic in process)

Step 2: Split image

Step 3: Halftone image- share1-share2

Step 4: Halftone image – reconstructed image(secret image)

The decryption phase is opposite to the encryption. The natural shares can share using the various media such as postal, email, or any other media. Retrieve the information from the combined image and the QR code. Transform the numeric value into binary form. Convert the binary string into resultant matrix. From the resultant matrix the corresponding reconstruct secret image can retrieve. Diagrammatic representation of proposed method is shown Below

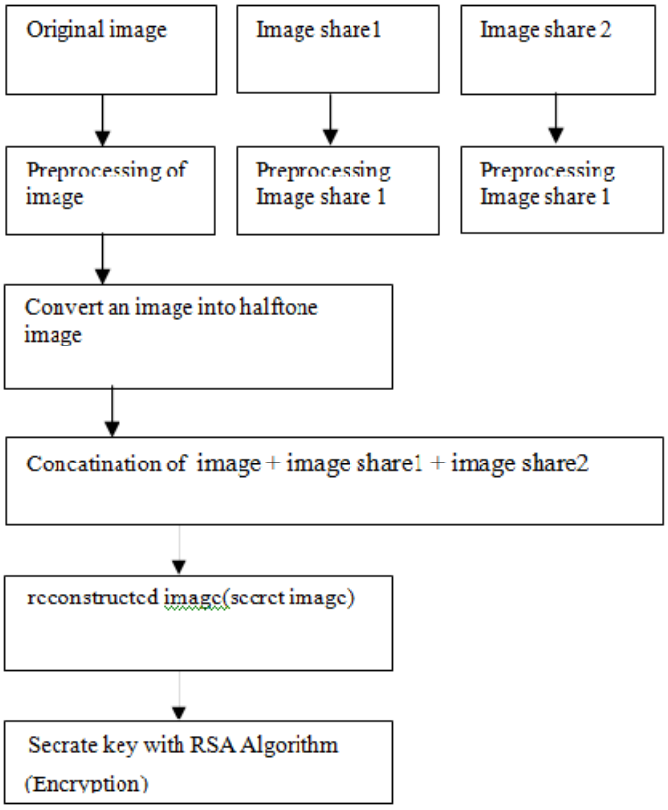

Fig 1: Secure big data sharing scheme using key storage

VII. OUTCOME AND POSSIBLE RESULTS

In this way the proposed method is performing for the secure transformation model when image moves out of network. With the help of the sharing images the proposed method encrypts secret image into two shares. Each share is indistinguishable from noise images, and so leaks no information about the secret.

VIII. CONCLUSION

This paper focused on the study of various secret sharing scheme i.e. Extended visual cryptographic schemes (EVCS), Visual secret sharing schemes for plural secret images (VSS-q- PI), Threshold multiple-secret visual cryptographic schemes (MVCS), Secret image sharing procedure, Secret image retrieving procedure, The Two-Phase Encryption Procedure. But there are some problems in secure image transmission so to improve this "secret image sharing with encryption decryption" sharing method for secure transmission is proposed here. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both forshares and for participants.

IX. FUTURE SCOPE

From observations of the proposed method the future work will include security analysis more simpler and more practical, reduce the transmission risk problem for participants and shares.

REFERENCES

1. Ching-Chun Chang, Yanjun Liu, Hsiao-Ling Wu, "Distortion-free secret image sharing method with two meaningful shadows", *IEEE TRANSACTIONS ON* Image Process., Vol. 10, Iss. 8, March 2016.

2. Kai-Hui Lee and Pei-Ling Chiu," Sharing Visual Secrets in Single Image Random Dot Stereograms", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 10, OCTOBER 2014.

3. Manami Sasaki and Yodai Watanabe, "Visual Secret Sharing Schemes Encrypting Multiple Images", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 13, NO. 2, FEBRUARY 2018.

4. Yodai Watanabe, Member, IEEE, "Visual Secret Sharing Schemes Encrypting Multiple Image", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 14, NO. 8, AUGUST 2015.

5. Pei-Ling Chiu," Sharing Visual Secrets in Single Image Random Dot Stereograms", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 10, OCTOBER 2014.