Secret Image Sharing Methodologies for Digital Communication Network: A Review

Amreen Bano Siddiqui[1], **Manoj Kumar**[2]
Computer Science department, LNCTS, Bhopal[1,2]

Abstract - Secret sharing is an important phenomenon in order to secure the data transmission. The secure transmission takes palace in digital world of the communication System. There are number of approaches have been proposed in the current scenario. There is some problem that may occur while reconstructing the data at the reconstruction site. In this manner this paper has been proposing an optimal approach in order to perform secret sharing. This paper is going to Propose an approach during review on the image processing that totally depend upon the threshold, where a secret image can be split into N small sub-files and combination of any T sub-files, the original file can be recovered without errors.

Keywords - Secret image, Secret sharing , Share building , Share distribution , Secret share reconstruction

1 INTRODUCTION

With rapid growth of computers and computer networks, enormous amount of digital data can easily be transmitted or stored over network. However, the intruders can easily sense or manipulate the confidential data transmitted over the networks by some cryptographic tools. So recently numerous of research has been carried in the field of information security and number of researcher work in the field of efficient secret sharing scheme.

In information security field, secret sharing is a process of distributing confidential massage among a set of participants, every participant have allocate a share of the secret .Then confidential massage can only be retrieved when all the participant combined together; individual shares are of no use on their own.

An image is an array, or a matrix, of square pixels (picture elements) arranged in columns and rows Image processing is one of the form of signal processing, in this input is an image, like video frame or a photograph; the output of image processing may be an image or, a set of features or parameters related to the image. Image processing refers to digital image processing but optical and analog image processing is also possible. There are different fundamental steps for image processing that are described below.

i. Image Acquisition:

This is the first step in image processing which perform by giving input as an image that is already in digital form. The image acquisition stage involves pre-processing, such as scaling etc.

ii. Image Enhancement:

Image enhancement is simplest and most interesting area of digital processing Where enhancement techniques is used to emphasize certain features of interest In an image, such as contrast & changing brightness etc.

iii. Image Restoration:

Image restoration improves the appearance of an image. Image restoration techniques based on mathematical or probabilistic models of image degradation.

iv. Colour Image Processing:

Due to increase in usage of digital images over the Internet, colour image processing is gaining importance. This may include colour modelling and processing in a digital domain etc.

v. Wavelets and Multi resolution Processing:

In Wavelets images are represented by various degrees of resolution. Here in this step images are sub divided into smaller regions for data compression and for pyramidal representation.

vi. Compression:

Due to usage of image in internet, compression is used to reduce the storage which is necessary to save an image or the bandwidth to transmit it.

vii. Morphological Processing:

Morphological processing tools used for extracting image components which are then use for representation and description of shape.

viii. Segmentation:

Segmentation is the process that split an image into small segments, which is done on the basis of some homogeneous criteria.

ix. Representation and Description:

In Representation and description, input is segmentation stage output, which usually is raw pixel data, which may be the points in the region itself or the boundary of a region. Representation is used to convert raw data into a form suitable for computer processing. Description extract attributes that effect in some quantitative information of interest or that may be used for differentiating one class of objet with other.

x. Object Recognition:

Recognition process is use to assigns a label.

xi. Knowledge Base:

Knowledge is the process that is used for detailing a region of image where the interest information is known to be located.

2 SECRET IMAGE SHARING SCHEME

In secret sharing scheme, due to security concern of confidential massage, it is required to divide secret massage (SM) into N subpart and share each part with N different host and retrieve the confidential massage by combining all N different part when required. Blackly [1] and Shamir [2] introduce secret sharing scheme first time in 1979. Moreover blackly secret sharing scheme cannot stop fake player to make participation during secret recovery and which lead to generate wrong message.

Recently researcher had presented numerous of method to make a control over such fake attempts [3]. Which broadly divide into two categories cheating detection and cheater identification. In cheating detection method, authorized members have to detect whether there exists a cheater in revealing the secret data or not [4].The second can be used to identify the cheater [3].

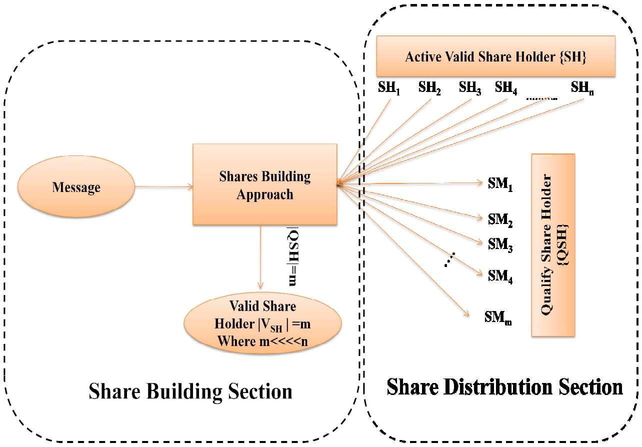
Active Valid Share Holder {SH}
SH_1
SH_2
SH_3
SH_4
SH_n
Message
Shares Building Approach
|QSH|=m
Valid Share Holder $|V_{SH}|$ =m Where m<<<<n
SM_1
SM_2
SM_3
SM_4
SM_m
Qualify Share Holder {QSH}
Share Building Section
Share Distribution Section

Figure 2:- Share Building and Distribution Phase

The basic idea of secret sharing is to divide information into several pieces such that certain subsets of these pieces (shares) can be used to recover the information. Where face player want to retrieve several shared information. In order to make participate in reconstruction of secret information and try to destroy the information.

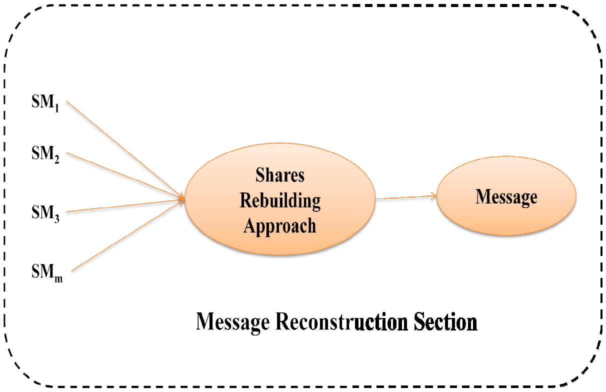

Figure 3:- Share Secret Reconstruction Phase

Secret sharing scheme having three different phases namely share building phase, share distribution phase and secret reconstruction phase. Along with that there is one secret update phase which is really used. Share building phase used to select share holder as QSH from participant set of share holder SH where cardinality of |QSH|= m and |SH|=n where m<<<n .as show in share building phase of figure 2.

Share distribution phase used to distribute each sub massage to each and every qualify share holder QSH as show in share distribution phase of figure 3.

Share building phase distribute all N different shadow image, then share recovery phase combine any random T phase to reconstruct original massage image.

$$\text{Original image} = SM^{X}{}_{1,T} + SM^{X}{}_{2,T} + SM^{X}{}_{3,T} +,,,,,,,,,+ SM^{X}{}_{T,T}$$

3 VISUAL SECRET SHARING

A visual secret sharing (VSS) scheme, which originates from the visual cryptography proposed by Naor-Shamir, may be one of the most well known realization of SS schemes.

The VSS scheme is a method to encode a secret image into several shares, each of which does not reveal any information of the secret image. Each share is printed on a transparency, and is distributed to one of n participants. The secret image can easily be decrypted only by stacking the shares in an arbitrary order. For instance, an example of a (k, n)-threshold VSS scheme is illustrated, Note that VSS schemes can be realized for not only (k, n)-threshold access structures but also general access structures. Furthermore, VSS schemes for color and/or gray-scale secret images can be constructed although the example which treats black-white (BW) binary secret image.

4 LITRETURE SUREVEY

The audio cryptography the optical cryptography and the cerebral cryptography are also SS schemes which use human senses in decryption in the same way as VSS schemes. In the audio and optical cryptography, a secret and shares are sounds or lights which can be considered as waves, and the interference of waves are used in decryption. In other words, the waves of shares corresponding to a qualified set are strengthened each other to listen to or to see the secret, but the waves of shares for a forbidden set are weakened each other to hide the secret. The audio cryptography is not unconditionally secure, although the tempo-based audio cryptography proposed in can guarantee unconditional security. In the tempo-based audio cryptography, secret bits are encrypted into rhythms, and security assumptions are similar to VSS schemes. The cerebral cryptography is a SS scheme based on the so-called stereogram. The stereogram is an illusion of eyesight that can perceive a 3-dimensional image from two 2-dimensional images. However, the security conditions are not clarified.

In other different approach, The first QSS scheme is a three-party protocol based on three entangled particles called Greenberger-Horne-Zeilinger (GHZ) state. In this QSS scheme, the measurement result for one share can be determined by combining measurement results for the other two shares. Hence, this method in can be considered as an extension of a quantum key sharing scheme rather than a QSS scheme. A (k, n)-threshold QSS scheme is considered in as an extension of the method in . In QSS schemes treated in secret information is ordinary bits which are encoded into quantum states. On the other hand, it is proposed in to encrypt a secret quantum state into shares. It is shown in that (k, n)-threshold QSS schemes can be realized

Here there is discussion of some authors who has been done their work in previous years.

In this paper the author [5] has presented a technique for multi-secret sharing. This approach has used recursive computational approach. The author works on multi-secret sharing approach in order to hide (k – 2) secrets. These secrets are of size b. This can be apply as a steganographiy. Here the steganographiy is use to convey the hidden information in order to perform the authentication and verification as well. Authentication and verification has apply on both contents which is shareable and secret also. In Further, the author would like to work on information on the Web, sensor networks and information dispersal schemes.

The rapid growth of mobile communication [6] there is a need to make new mobile phone having attractive features. With this aim the mobile phone give the facility of photo sharing which is very popular among the users. In this paper the Author has proposed an efficient algorithm which is use for the photo sharing with preserving privacy of the user. This may work on the small photos but it efficient. The model provided by the author has worked with respect to facebook also. Here the P3 have not required any changes in the present scenario or the software of the mobile phone. As per the author it may possible of some overhead in the work.

Secret sharing [7] is an approach in order to spread the a secret to the collection of participants, each of whom is allocated with a share of the secret. The actions of the participant are used to reconstruct the secret. Simple individual participants' action is useless. Sharing systems reversible images and threshold approach is used to achieve novel sharing secret color images. Secret image pixels colors will be converted to rating system of order m. In this work the Quantization process has applied by the author in order to enhance the quality of the image. Peak signal to noise ratio has also calculated in order to examine the quality of the output images. The result of the proposed work shows that the outcomes are lossless.

The purpose of author [8] for exchange is to embed a secret image and the cover image to reduce image distortion shade. The most important aspect of recovery reconstructs the lost secret picture. Many existing schemes work well for the first task, but most fail to recover the secret image successfully. To solve this problem, a new method for sharing secret image based on a field power of two Galois instead of prime numbers is proposed. Our experimental results show that our system provides shadow images of satisfactory quality, although it can properly reconstruct the secret image and cover with lossless image

As [9]per the author two famous author Naor and Shamir firstly has introduced the secret sharing in the early 90's. they started the image sharing with the binary image. The author has a proposed a approach which uses the Hill cipher method hiding the data. Apart from that one more approach also has used random grid. In this approach it seems to be that pixel expansion rate has been decrees and image recovery has been lossless. The experimental result was far better than the previous approach.

5 PROBLEM FORMULATION

With rapid growth of computers and computer networks, enormous amount of digital data can easily be transmitted or stored over network. However, the intruders can easily sense or manipulate the confidential data transmitted over the networks by some cryptographic tools. So recently numerous of research has been carried in the field of information security and number of researcher work in the field of efficient secret sharing scheme.

6 PROPOSED APPROACH

Proposed methodology will use to split the secret massage image SMI into N different shadow image like SMI1, SMI2, SMI3 ……. SMIn at sending end . Whereas at receiving end original image can be recover by combining T (T<<<N) different shadow image. In order to achieve this goal proposed work is divided into two phases secret sharing and secret recovery.

7 EXPECTED OUTCOMES

Proposed methodology will use any random and minimized T subparts to reconstruct original image message in place of N subpart. This way proposed methodology avoids using fake player to make participate in image reconstruction. Along with that proposed methodology will be quit faster than existing one as it requires only T subpart to combine which is very less than N.

8 CONCLUSION

This paper is a literature review on a secret sharing schemes and going to introduce optimal threshold schemes which is based on prime number just greater than pixel value of original image. This paper has discussed the various previous approaches by which the secret image sharing is possible. These techniques are useful in gray scale image. This paper also suggested the approach by which the image sharing is efficiently done.

9 REFERENCE

[1]. Blakley, G.R.: 'Safeguarding cryptographic keys'. Proc. AFIPS National Computer Conf., 1979, vol. 48, pp. 313–317

[2]. Shamir, A.: 'How to share a secret', Commun. ACM, 1979, 22, (11), pp. 612–613

[3]. Hu, C.M., Tzeng, W.G.: 'Cheating prevention in visual cryptography', IEEE Trans. Image Process., 16, (1), pp. 36–45,2007

[4]. Zhao, R., Zhao, J.J., Dai, F., Zhao, F.Q.: 'A new image secret sharing scheme to identify cheaters', Comput. Stand. Interfaces, 31, (1), pp. 252–257,2009

[5]. Abhishek Parakh and Subhash Kak, "Recursive Secret Sharing for Distributed Storage and Information Hiding", ACM 2009 Proceedings of the 3rd international conference on Advanced networks and telecommunication systems, pp 88-90

[6]. Moo-Ryong Ra, Ramesh Govindan and Antonio Ortega, "P3: Toward Privacy-Preserving Photo Sharing" 10th USENIX Symposium on Networked Systems Design and Implementation 2013, pp 515-528.

[7]. Anbarasi, L.J. and Kannan, S.," Secured secret color image sharing with steganography", IEEE 2012, pp 44 - 48

[8]. Ming-Chun Chien and Hwang, J.G., "Secret image sharing using (t,n) threshold scheme with lossless recovery", IEEE 2012, pp 1325 - 1329

[9]. Wei-Kuei Chen, "Image sharing method for gray-level images", The Journal of Systems and Software 86, Elsevier 2013 pp 581–585

[10]. Ching-Nung Yang, Tse-Shih Chen , "Improvements of image sharing with steganography and authentication" in Journal of Systems and Software 80 , Elsevier 2013, pp 1070–1076,