JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# Review paper on secret sharing scheme for hiding data

**[1]Sakshi N. Sable, [2] Dr. Prashant R. Deshmukh,**

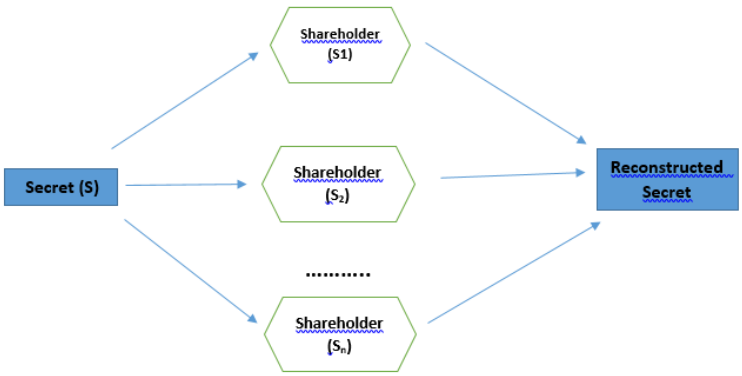
[1]Mtech Student, [2]Head of Department
[1]Electronics and System Communication Engineering
[1]Government College Of Engineering, Amravati, India

*Abstract :* Over the past few years, communication technology has faced significant concerns over information security. The key issue has been how to keep information private while verifying it and guarding against it being changed before it reaches the recipient. One component of the solution to these issues is cryptography. Using mathematical techniques, the goal of cryptography is to prevent unwanted access to or modification of data. This is accomplished via a shared secret key in symmetric cryptosystems and a pair of keys, public and private, in asymmetric cryptosystems. The usage of secret keys or public-private key pairs brought up the issue of how to store them safely. Most often, traditional cryptology is used to prevent data from being manipulated, but decoding requires complicated computation. Secret sharing algorithms for covering data that provide risk-free, dependable storage and enhance security are used to decrease computation while also improving data security.

***Keywords*** - Secret sharing, cryptography, secret key.

## I. INTRODUCTION

As the network becomes more and more popular, hackers use Internet leaks to acquire the data they're after. Secure data transmission therefore becomes necessary. Secret sharing explains cryptographic techniques for dividing a secret into many shares and giving each share to a different party; the secret can only be recovered when all the parties bring their individual shares together. In more detail, the holder of a secret, also known as the dealer, produces n shares of the secret and sets a threshold t for the quantity of shares needed to reconstruct the secret. The dealer then distributes the shares such that they are held by various parties An enemy who obtains access to fewer shares of the secret than the threshold cannot learn the secret in safe secret sharing techniques. Because they enable more secure storage of highly sensitive data, such as encryption keys, missile launch codes, and digital bank accounts, secret sharing systems are beneficial. The data is divided so that there is not a single point of failure that could cause it to be lost. A secret sharing system offers ease, security, and consistency.




Safety of cryptographic keys and safe information storage were the driving forces behind secret sharing. A key or piece of information can be safely kept in several storage locations as shares and recovered when required.

## II. LITERATURE REVIEW

In this part, a review of related research in the subject of visual cryptography is provided. To exchange a secret image among n people, Naor and Shamir originally came up with the Visual Secret Sharing (VSS) technique. To create many shares, they have created basis matrices. Basis matrices, which are made up of a number of ones and zeros, are used to divide up secret image pixels into different portions. Many experts have developed VSS-based methods that can recover the hidden image with up to 50% contrast over the years.

In [2] Adi Shamir a secret sharing scheme utilising a polynomial-based method. The idea behind this approach is that by evaluating polynomial equations, the secret is separated into a number of pieces. Reconstruct the secret using the Lagrange interpolation approach in this scheme. This method implements a scheme, where is the threshold, or the total number of participating members. A minimum number of Participants must submit a secret in order to receive the original secret, but less Participants must submit a secret of sharing in order to remain in the dark regarding the original secret.

In [3] Leelavathi Rudraksha et al. for secure data transfer introduced a unique visual cryptography approach with k-n secret sharing that is then hidden in package cover pictures utilising LSB technique. A random number generator algorithm is used to generate inputs for the generation of shares since the creation of n shares requires the input of random data. Comparatively speaking to other existing methods of visual cryptography on colour images, this technique requires extremely little mathematical calculation.

Many cryptographic encryption algorithms were developed in [4] Sonal Kukreja et al. to secure the secret image. The Visual Secret Sharing Scheme is a very secure encryption method with the added benefit of requiring no decryption method; the secret image can only be unlocked using the human visual system. The majority of Visual Secret Sharing Schemes (VC) schemes in use today do not offer effective authentication capabilities, and those that do either suffer from pixel expansion or have a low detection rate. Additionally, the meaningless shares and poor visual quality of the received secret image plague Random Grid (RG) based VC schemes. These flaws were taken into account and fixed in the suggested work. These problems were taken into consideration and fixed in the suggested work. A model (k,n) visual secret sharing technique with more authentication options has been put out. The secret image is used to create n random grids, to which the authentication bits are then inserted. The SHA-256 cryptographic hash function, which is quite effective, is used to generate the authentication bits. These shares are then transformed into informative share images, which are easier to manage and guarantee security. The consistency of the authentication codes for all shared photos is checked at the time of retrieval, which aids in determining whether or not the received image has been altered. The recovery of hidden information is prohibited if it has been tampered with; otherwise, k out of n share photos are overlay to retrieve the hidden image. XOR operation was used to increase the contrast of the hidden image that was received at the moment of superimposition. The suggested method demonstrates that it is a reliable and safe visual secret sharing method for image authentication. The experimental findings have been used to demonstrate and prove the viability of the proposed plan.

The concept of secret sharing was first proposed by Sonali patil and Prashant Deshmukh [8]. The dealer divides the secret into shares, which are subsequently dispersed to the participants. Reconstruction of the original secret is only possible for specific approved subsets of participants. Applications for anonymous sharing networks appear to be becoming more significant these days. Secret sharing needs to offer more capability and flexibility in many situations to meet the demands of an application. For many years, secret sharing has been a topic of active investigation. The need to implement a secret sharing scheme with all augmented capabilities, such as general access structure, robustness against cheating shareholders, verifiability of the shares, proactive redistribution of shares, etc., is evident despite the development of numerous secret sharing techniques to secure data.

Ms. K. Chitra et.al [6] have proposed the modern secret sharing scheme has been proposed as a development of the conventional secret sharing scheme based on the use of technology. The fundamental contrast between Visual cryptography and the established secret sharing technique is presented. Pixel sharing patterns and its procedure have been discussed in relation to the explanation of the image-based share creation method. The XOR/OR Boolean operation is used to produce the reconstruction image. Mathematical explanations of threshold-based share generation techniques are provided, along with a comparison of these schemes.

The secret sharing technique has significantly improved over the last three decades to provide better image security. Adi Shamir invented the SS technique in the form of a physical paper to conceal the data using transparent sheets. Later, for greater security, Adi Shamir and Moni Naor enhanced the SS technique [9]. The development of visual cryptography as a method of data protection came about as a result of technological innovation and the widespread use of electronic devices. In following table there is comparison between visual cryptography and the conventional secret sharing method illustrates the key distinctions between the two addressed the majority of the significant disparities; their names are listed in the tabular column.

| Traditional Secret Sharing Scheme | Visual Cryptography |
|---|---|
| The lesser amount of secret is embedded | It encrypts a huge amount of secret information |
| Codebook is required | Polynomial based sharing scheme in visual cryptography requires codebook. |
| Facing alignment problem while decrypting the secrets | Boolean operation-based decryption nullifies the alignment problem |

| | |
|---|---|
| The generation of shares is based on the threshold level | The generation of shares is based on binary values |
| Secret sharing scheme is derived from cryptographic concepts. | Visual cryptography is derived from the secret sharing scheme. |
| Cost of computing is high for transmitting and storing the information. | Cost of computing is low while transmitting and storing the information. |
| The problem arises in a secret sharing scheme is Space-efficient, robustness, contrast, etc. | Contrast problem only arises in this scheme. |
| Does the sharing process for text messages. | Does the sharing process for images, later it spread into all multimedia contents. |

## III. RESEARCH METHODOLOGY

The suggested methodology takes into account two goals for the experiment. Automate the decision-making threshold for similarity measurement first, and then improve the accuracy of the authentication process. The authentication system method consists of two steps.

1. Enrolment
2. Authentication

Images (cover image and secret image) are taken during the enrollment procedure. To reduce noise, normalisation is applied to the data after the photos are taken. The significant texture characteristics are extracted from the photos using the transform domain, and a feature vector is created. The photographs will then be combined using an image fusion technique to create a single image that includes both the dealer's and the secret image. Thus, the feature vector is divided into 'n' shares using a secret sharing technique. It could be shared or kept.

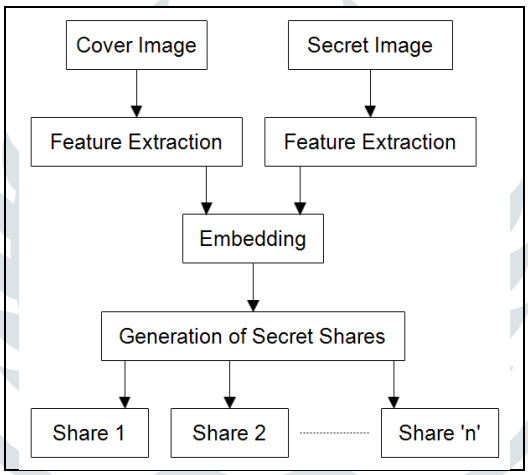



Fig: Enrollment Process

The distribution of the 'n' shares occurs throughout the authentication process. A certain number of those "k" shares are delivered to the receiver. Images are rebuilt using templet reconstruction after obtaining shares. As a result, the Fused Image is rebuilt. The key texture characteristics are extracted from the fused pictures using the inverse transform domain, and a feature vector is created. As a result, photos containing protected data (secret images) are retrieved.

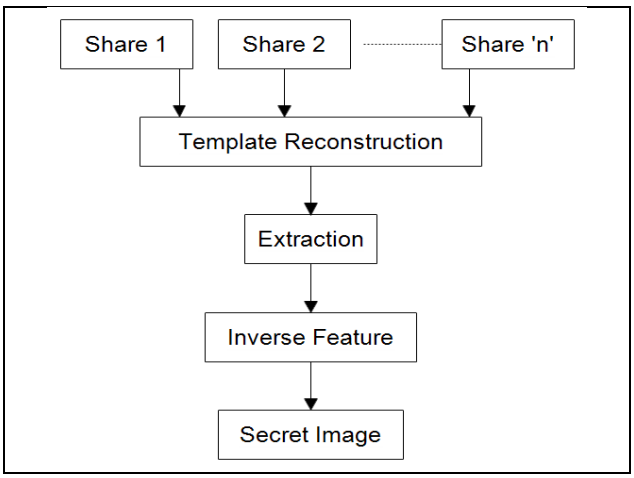



Fig: Authentication Process

## IV. CONCLUSION

This idea has made cryptography considerably simpler to implement without needing any complicated keys, according to research on several visual cryptography schemes. Progressive visual cryptography avoids the issue of pixel expansion, but (k, n) threshold technique has excessive pixel expansion. The paper suggests a secret sharing-based safe authentication method. The suggested solution is highly helpful in boosting the authentication system's security against threats made on centralised databases. Using secret sharing, the database is decentralised in a safe manner. The suggested method uses a transform domain to extract features, which helps to conceal the information about the traits.

## REFERENCES


**[1]** Shruthy Sasidharan , Preethi Bhaskaran , Jayanthi V S (2018). "Enhanced Security of Sensitive Images by Cryptography and Hiding Methods."

**[2]** Shamir, "How to Share a Secret," *Communications of ACM, vol. 22,* pp. 612-613, 1979.

**[3]** Leelavathi Rudraksha giri prasad m.n (2019) "Advanced robust data hiding using visual cryptography.

**[4]** Sonal Kukreja Singara Singh Kasana Geeta Kasana (2018) " Random Grid based Extended Visual Secret Sharing Scheme for Image Authentication."

**[5]** Pei-Fang Tsai, Ming-Shi Wang. "An (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data..

**[6]** Ms. K. Chitra , Dr. V. Prasanna venkatesan (2020). "An Antiquity to the contemporary of Secret Sharing Scheme."

**[7]** Sonal Kukreja, Geeta Kasana (2019). "Secure Reversible Data Hiding Scheme for Digital Images using Random Grid Visual Secret Sharing Linear."

**[8]** SonaliPatil, PrashantDeshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications, vol. 46, No. 19, pp. 610, 2012.

**[9]** M. Naor and A. Shamir, "Visual cryptography," in Workshop on the Theory and Application of of Cryptographic Techniques, pp. 1–12, Springer, 1994.

**[10]** Aaqib Anjum Reshi Shabir A. Parah (2018) "Performance Evaluation and Future Scope of Image Secret Sharing Schemes."

**[11]** Nileshkumar Kakade , Utpalkumar Patel (2020). "Secure Secret Sharing Using Homomorphic Encryption ."

**[12]** Persis Saro Bell. N Mrs.L.R.Priya , Santhana Lakshmi.N (2018). "Secure Data Hiding Based on Most Significant Bit Error Prediction Mechanism using Blow Fish Algorithm."

**[13]** Binu V., P Sreekumar A (2015)."Simple and Efficient Secret Sharing Schemes for Sharing Data and Image"