

SECRET IMAGE SHARING SCHEMES THROUGH SIS

Nazima Begum¹, T. Anita², Prof B V Ramana Murthy³

¹PG Student, Computer Science & Engineering ISL Engineering College, India

²Assistant Professor, Department of Computer Science & Engineering, ISL Engineering College, India.

³Professor, Department of Computer Science & Engineering, Stanley College of Engineering & Technology for women.

DOI: [https://doi.org/10.63001/tbs.2024.v19.i02.S.I\(1\).pp753-759](https://doi.org/10.63001/tbs.2024.v19.i02.S.I(1).pp753-759)

KEYWORDS

SIS,
VSIS,
Secret Image.

Received on:

19-09-2024

Accepted on:

23-12-2024

ABSTRACT

The safeguarding of digitized data against unwanted access and modification has become an issue of utmost importance as a direct result of the rapid development of network technology and internet applications. In response to this challenge, numerous secret image sharing (SIS) schemes have been developed. SIS is a method for protecting sensitive digital images from unauthorized access and alteration. The secret image is fragmented into a large number of arbitrary shares, each of which is designed to prevent the disclosure of any information to the trespassers. In this paper, we present a comprehensive survey of SIS schemes along with their pros and cons. We review various existing verifiable secret image sharing (VSIS) schemes that are immune to different types of cheating. Additionally, we discuss steganography techniques that hide secret information within digital images and Shamir secret sharing, which divides a secret into multiple parts, with a threshold number of parts required to reconstruct the secret. We have identified various aspects of developing secure and efficient SIS schemes, including steganography and Shamir secret sharing. In addition to that, a comparison and contrast of several SIS methodologies based on various properties is included in this survey work. We also highlight some of the applications based on SIS. Finally, we present open challenges and future directions in the field of SIS.

INTRODUCTION

The fast progression of network technology and internet applications has created an urgent need to protect digital data from illegal access and alteration. A vital component of data protection is the safeguarding of sensitive digital pictures, resulting in the creation of several secret image sharing (SIS) methods. These techniques partition confidential photos into several shares to prevent illegal disclosure and modification. In conjunction with SIS, methodologies such as steganography, which conceals confidential information inside digital pictures, and Shamir secret sharing, which partitions secrets into many components, are crucial in augmenting data security. This study presents a thorough examination of SIS systems, including verified secret image sharing (VSIS) techniques that counter various types of cheating. We examine the amalgamation of steganography and Shamir secret sharing inside SIS techniques, evaluate their advantages and disadvantages, compare diverse SIS schemes based on distinct characteristics, explain practical applications, and delineate unresolved obstacles and prospective avenues in this advancing domain.

LITERATURE REVIEW

S. Dey., SD-El: A cryptographic technique to encrypt images, This study introduces SD-El, a cryptographic method explicitly formulated for image encryption. It tackles the specific difficulties associated with picture data security, including the preservation of confidentiality, integrity, and resilience against assaults. The approach utilizes a blend of encryption algorithms and image processing techniques to guarantee the safe encryption and decryption of pictures. It was presented at the International Conference on Cyber Security, Cyber Warfare, and Digital

Forensics in June 2012, underscoring its significance in the fields of cybersecurity and digital forensics.

Q.-A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, N. N. Quaynor., A cryptographic technique for security of medical images in health information systems. This work introduces a cryptographic method particularly designed to secure medical pictures in health information systems. The method mitigates privacy and security issues related to medical imaging data, safeguarding confidentiality and integrity during storage, transmission, and access. It examines cryptographic methods, key management techniques, and access control systems to protect medical pictures in hospital settings. Published in the Proceedings of Computer Science in January 2015, it demonstrates its significance to health informatics and data security.

M. Mundher, D. Muhamad, A. Rehman, T. Saba, F. Kausar., Digital watermarking for images security using discrete slantlet transform. Digital watermarking methods for picture security that make use of the discrete slantlet transform are investigated in this study. Improving security, copyright protection, and authenticity verification via the introduction of barely noticeable watermarks into photos is its primary emphasis. Embedding and extracting watermarks, as well as their resilience against assaults and applications in protecting multimedia material, are the topics covered in this study. This article aids in the preservation of intellectual property and digital rights and was published in the November 2014 issue of Applied Mathematics and Information Sciences.

A. Mohanarathnam., Digital watermarking techniques for image security: A review, This review article offers a comprehensive analysis of digital watermarking approaches focused on picture security. This document examines many watermarking methodologies, including spatial domain, frequency domain, and

transform domain approaches, while emphasizing their advantages, disadvantages, and applications. The document examines progress in watermarking techniques, resilience to assaults, and their integration with encryption to improve picture security. Published in the Journal of Ambient Intelligence and Humanized Computing in 2020, the review provides significant insights for scholars and practitioners in the domain of image security.

A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt., Digital image steganography: Survey and analysis of current methods. This study provides an extensive overview and analysis of contemporary digital picture steganography techniques. It encompasses several steganographic techniques used for the concealment of information inside digital pictures, including LSB embedding, frequency domain approaches, and adaptive steganography. The document examines the advantages and disadvantages of each method, their detectability, and their uses in clandestine communication and data concealment. Published in March 2010 in Signal Processing, the survey serves as a helpful resource for comprehending the current advancements in digital picture steganography.

M. Idakwo, M. Muazu, E. Adedokun, B. Sadiq., An extensive survey of digital image steganography: State of the art. This survey paper provides a comprehensive examination of digital image steganography techniques, detailing the current advancements in concealing information within digital images. The text examines the progression of steganography, highlights recent developments in steganographic techniques, and addresses the challenges faced in steganalysis. This paper examines various aspects, including resilience to attacks, the ability for data concealment, and the implications for multimedia security. The survey, published in the ATBU Journal of Science, Technology, and Education in 2020, synthesizes existing knowledge and trends in the field of digital image steganography.

PROPOSED SYSTEM

Techniques for secret picture communication may safeguard these photos from potential dangers, making them a significant field of study. Although several earlier surveys have concentrated on certain SIS approaches or applications, there is a lack of comprehensive surveys that provide a holistic perspective on this domain. Although prior surveys and studies have concentrated on certain facets of SIS, including specific approaches or applications, a complete study offering a holistic perspective of the whole discipline is still necessary. The initial secret is divided into many shares via polynomial interpolation methods. Each share comprises a segment of the confidential information. A minimum threshold of shares, often established during the setup,

is necessary to reconstruct the secret. The amalgamation of the requisite number of shares using polynomial reconstruction facilitates the retrieval of the original secret. Shamir's Secret Sharing Scheme is extensively used in several applications requiring the safe distribution of sensitive information, including cryptographic key management, secure authentication procedures, and data backup systems. Steganography is the technique of hiding confidential information inside non-confidential material, such as digital photographs, audio files, or text. In contrast to encryption, which seeks to make data inaccessible to unauthorized individuals, steganography concentrates on concealing the very presence of the clandestine communication.

PROJECT DESCRIPTION

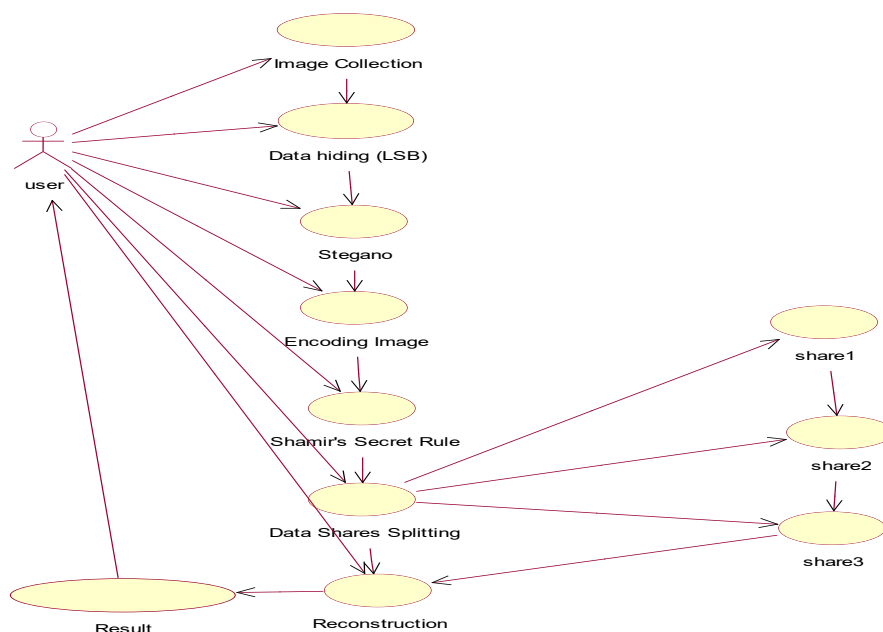
The project seeks to carry out an in-depth exploration of secret image sharing schemes, concentrating particularly on verifiable secret image sharing techniques, steganography methods, and Shamir secret sharing algorithms. The main goal is to create and execute advanced SIS schemes that combine steganography with Shamir secret sharing techniques, thus improving the security of digital image protection from unauthorized access and alterations. The project encompasses a thorough assessment of the performance and security metrics of the newly developed SIS schemes, taking into account aspects like encryption/decryption speed, resistance to attacks, and scalability. It is essential to analyze and evaluate these schemes alongside current ones to discern their advantages and disadvantages regarding security strength, computational efficiency, and real-world applicability. Additionally, the project seeks to investigate the practical uses of SIS schemes across multiple fields, including secure image sharing platforms, healthcare data protection, multimedia communication, and digital rights management (DRM). The project aims to tackle existing challenges in SIS, steganography, and Shamir secret sharing, proposing novel solutions and research pathways to enhance the security, efficiency, and usability of these techniques for future advancements and applications.

DESIGN ENGINEERING

Design Engineering involves the use of numerous UML (Unified Modeling Language) diagrams for project execution. Design is a significant engineering depiction of an object intended for construction. program design is a process that converts requirements into a representation of the program. Design is the domain in which quality is manifested in software engineering.

UML DIAGRAMS

USE CASE DIAGRAM

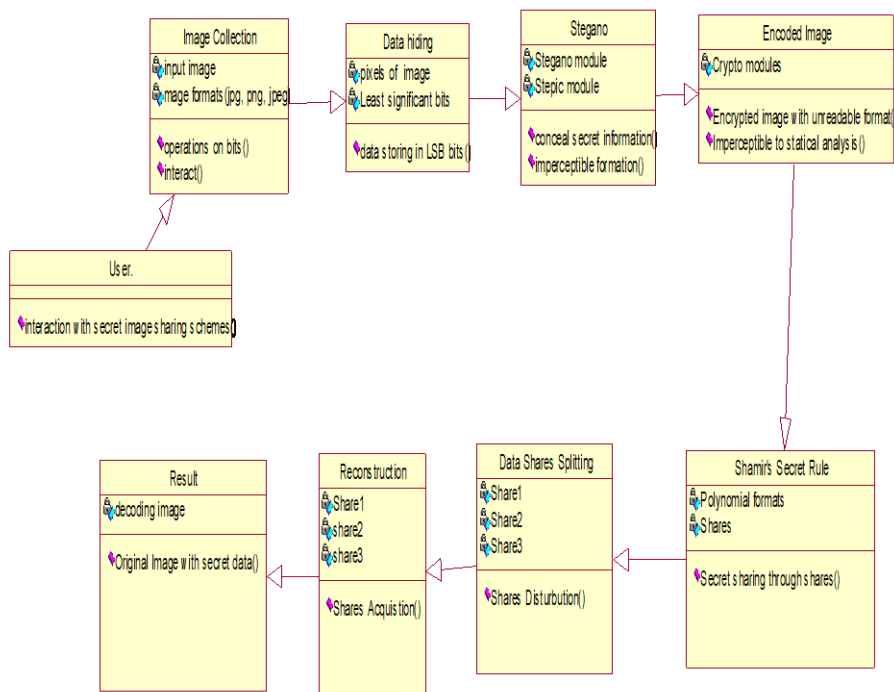


EXPLANATION:

The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the

system can be depicted. The above diagram consists of user as actor. Each will play a certain role to achieve the concept.

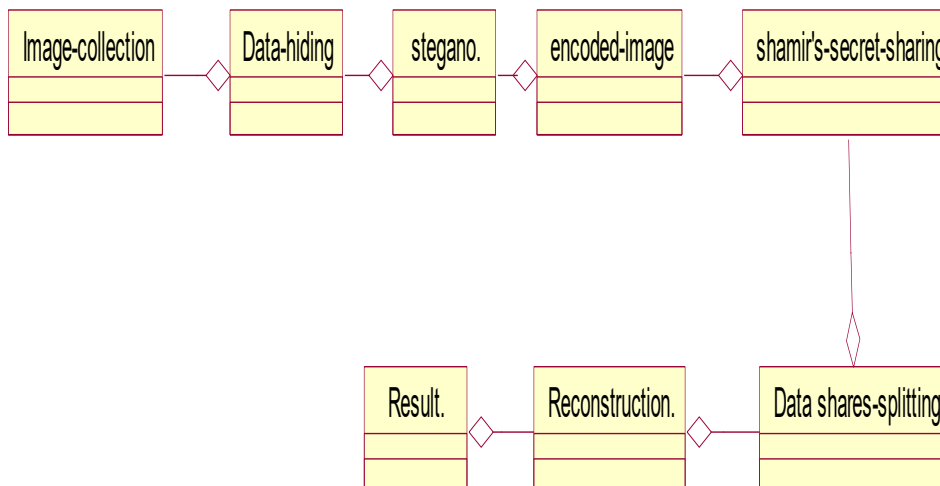
CLASS DIAGRAM



EXPLANATION

In this class diagram represents how the classes with attributes and methods are linked together to perform the verification with

OBJECT DIAGRAM



EXPLANATION:

In the above digram tells about the flow of objects between the classes. It is a diagram that shows a complete or partial view of the structure of a modeled system. In this object diagram

security. From the above diagram shown the various classes involved in our project.

represents how the classes with attributes and methods are linked together to perform the verification with security.

SYSTEM ARCHITECTURE:

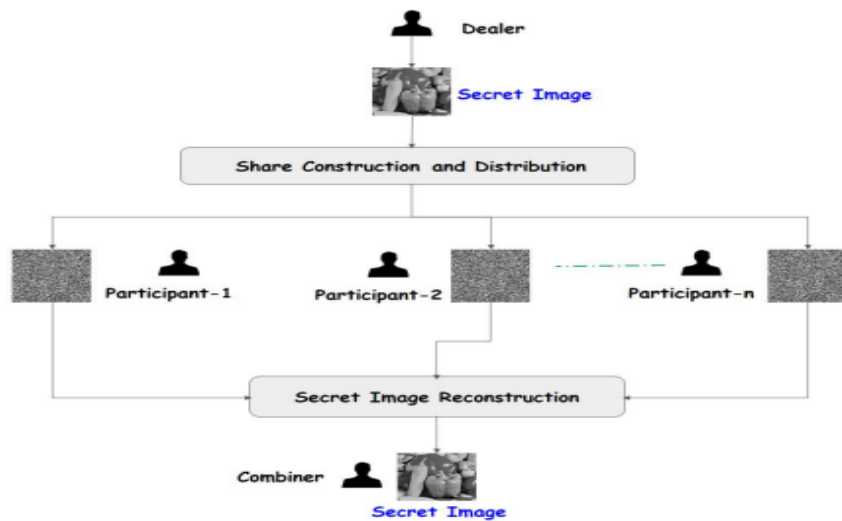


Fig 1: Proposed Model

SNAPSHOTS

SIS, Shamir's Secret Sharing, and steganography approaches assist enterprises in adhering to privacy rules by assuring secrecy and secure communication, therefore safeguarding sensitive information from unwanted access or exposure.

- SNAPSHOTS
- Secret Image sharing login page:

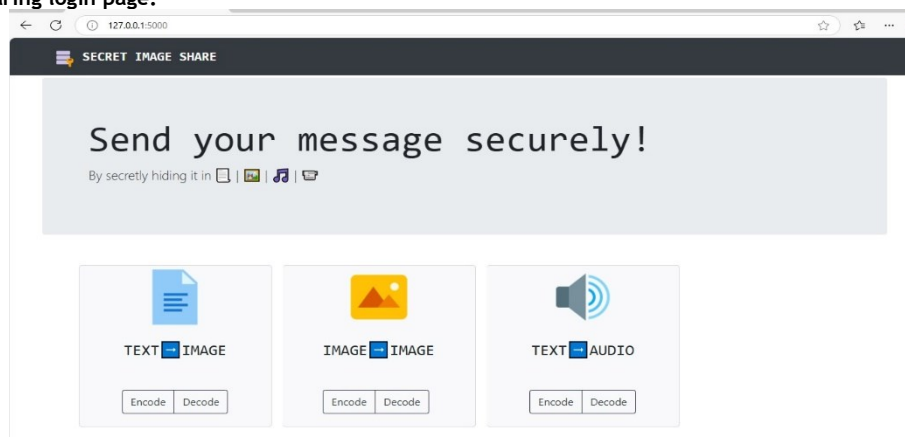


Figure 2: 1S ecret Image sharing login page:

Encode of Text to Image

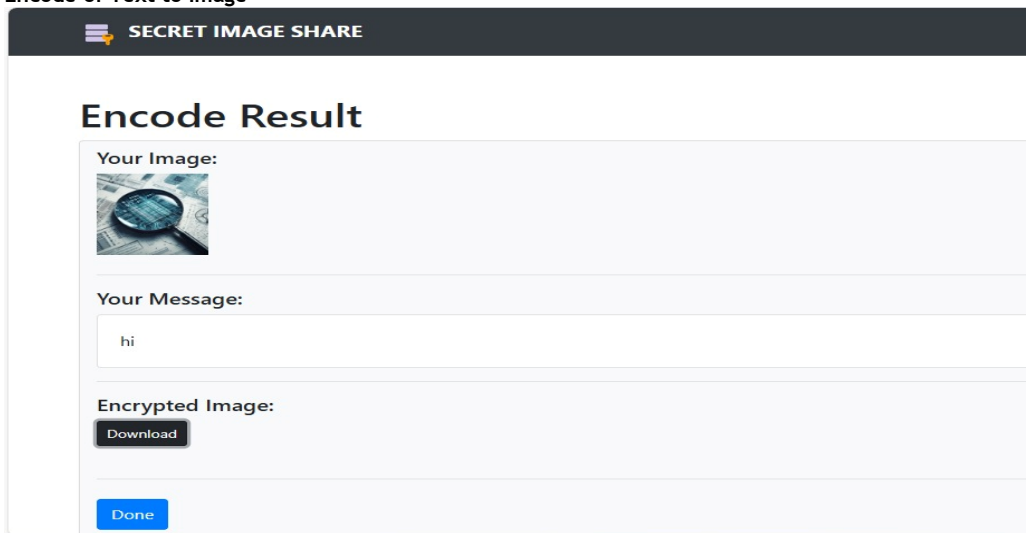




Figure 3: 2Encode of Text to Image

 SECRET IMAGE SHARE

Decode Result


Your secret message:

 Copy text

hi


Done

Figure 4 3Encode of Text to Image


 SECRET IMAGE SHARE

Encode Result

Your image:




Your Encrypted image:



Download

Done

Figure 5: Encode of Image to text:

 SECRET IMAGE SHARE

Decode Result


Your secret Image:

Download

done

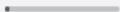


Figure 6: Decode of Image to text:

Encode of text to audio:

 **SECRET IMAGE SHARE**

Encode Result

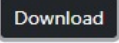
Your Audio:

▶ 0:00 / 2:36   

Your Message:

hii

Encrypted Audio:








Figure 7: Encode of text to audio:

Encode of text to audio:

 **SECRET IMAGE SHARE**

Decode Result

Your secret message:

 Copy text

Hi nazima




Figure8: Encode of text to audio:

SOFTWARE TESTING

The objective of testing is to identify mistakes. Testing is the procedure aimed at identifying any potential defects or vulnerabilities in a work product. It offers a method to assess the functioning of components, subassemblies, assemblies, and/or a

completed product. The process of testing software to ensure that the system fulfills its requirements and user expectations, while avoiding undesirable failures. There are several categories of tests. Each test category fulfills a distinct testing need.

FUTURE ENHANCEMENT

Advanced Steganography Techniques: Examine and use sophisticated steganography techniques beyond least significant bit (LSB) steganography, including spread spectrum methods, transform domain steganography, or adaptive steganography approaches. These strategies may provide enhanced security, increased data concealment capability, and resilience to steganalysis.

Quantum-Safe Cryptography: Examine the incorporation of quantum-resistant cryptography methods and methodologies inside the SIS and secret sharing paradigm. This entails investigating post-quantum cryptography techniques to guarantee robustness against future quantum computer assaults[17].

Dynamic Threshold Adjustments: Establish systems for the dynamic adjustment of the share threshold necessary for secret reconstruction, contingent upon the security context, risk considerations, or evolving surroundings. This may improve responsiveness and security in dynamic situations.

Multi-Modal Data Hiding: Expand the project to provide multi-modal data concealment, whereby confidential information is embedded throughout several forms of digital media (e.g., photos, audio, video) concurrently. This may provide improved security and resilience in multimedia communication and data protection.

Blockchain-Based Verification: Examine the use of blockchain technology for validating the integrity and validity of shared secrets and rebuilt pictures in Visual Secret Sharing (VSS) schemes. Blockchain-based verification may enhance confidence and provide tamper-resistance in the secret sharing process.

CONCLUSION

This study has explored the complex domain of secret image sharing (SIS) schemes, steganographic techniques, and Shamir secret sharing algorithms. We have developed and executed innovative SIS systems that combine steganography with Shamir secret sharing principles, therefore improving the security of digital picture protection against unwanted access and alteration. Our assessment of these newly devised systems has highlighted their performance, security standards, and computational efficiency, establishing a basis for comparison study with current SIS schemes. Through the examination of actual applications in secure picture sharing platforms, healthcare data security, multimedia communication, and digital rights management (DRM), we have shown the adaptability and usefulness of SIS approaches in real-world contexts. Future advancements may concentrate on sophisticated steganography methods, quantum-resistant cryptography, adaptive threshold modifications, multi-modal data concealment, blockchain-based validation, machine learning for steganalysis, intuitive user interfaces, and standards for interoperability. These initiatives will enhance progress in safe data exchange, encryption methodologies, and information security protocols, fostering a more robust and secure digital environment.

REFERENCES

- S. Dey, "SD-El: A cryptographic technique to encrypt images," in Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec), Jun. 2012, pp. 28-32.
- Q.-A. Kester, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, and N. N. Quaynor, "A cryptographic technique for security of medical images in health information systems," Proc. Comput. Sci., vol. 58, pp. 538-543, Jan. 2015.
- M. Mundher, D. Muhamad, A. Rehman, T. Saba, and F. Kausar, "Digital watermarking for images security using discrete slantlet transform," Appl. Math. Inf. Sci., vol. 8, no. 6, pp. 2823-2830, Nov. 2014.
- A. Mohanarathinam, "Digital watermarking techniques for image security: A review," J. Ambient Intell. Humanized Comput., vol. 11, no. 8, pp. 3221-3229, 2020.
- A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, no. 3, pp. 727-752, Mar. 2010.
- M. Idakwo, M. Muazu, E. Adedokun, and B. Sadiq, "An extensive survey of digital image steganography: State of the art," ATBU J. Sci., Technol. Educ., vol. 8, no. 2, pp. 40-54, 2020.
- A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612-613, Nov. 1979.
- G. R. Blakley, "Safeguarding cryptographic keys," in Proc. Int. Workshop Manag. Requirements Knowl. (MARK), 1979, pp. 313-318.
- M. Mignotte, "How to share a secret," in Proc. Workshop Cryptogr. Cham, Switzerland: Springer, 1982, pp. 371-375.
- C. Asmuth and J. Bloom, "A modular approach to key safeguarding," IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 208-210, Mar. 1983.
- C. S. Chum, B. Fine, G. Rosenberger, and X. Zhang, "A proposed alternative to the Shamir secret sharing scheme," Contemp. Math., vol. 582, pp. 47-50, Jan. 2012.
- K. E. Atkinson, An Introduction to Numerical Analysis. Hoboken, NJ, USA: Wiley, 2008.
- B. Fine, A. I. S. Moldenhauer, and G. Rosenberger, "A secret sharing scheme based on the closest vector theorem and a modification to a private key cryptosystem," Groups-Complex.-Cryptol., vol. 5, no. 2, pp. 223-238, Jan. 2013.
- Dr. Abdul Bari, Dr. Imtiyaz Khan, Dr. Rafath Samrin, Dr. Akhil Khare, "VPC & Public Cloud Optimal Performance in Cloud Environment", Educational Administration: Theory and Practice, ISSN No : 2148-2403 Vol 30- Issue -6 June 2024.
- C.-C. Thien and J.-C. Lin, "Secret image sharing," Comput. Graph., vol. 26, no. 5, pp. 765-770, Oct. 2002.
- J. Zhao, J. Zhang, and R. Zhao, "A practical verifiable multisecret sharing scheme," Comput. Standards Interface, vol. 29, no. 1, pp. 138-141, Jan. 2007.
- L. Ham and C. Lin, "Detection and identification of cheaters in (t, n) secret sharing scheme," Des., Codes Cryptogr., vol. 52, no. 1, pp. 15-24, Jul. 2009.