Secret Image Sharing Schemes

[1] Umme Ayesha, [2] Dr. B. Sasi Kumar

[1]M. Tech Student -CSE, Department of Computer Science Engineering, Dr. V.R.K Women's College of Engineering & Technology, Hyderabad, Telangana, India.
[2] Principal & Professor, Department of Computer Science Engineering, Dr. V.R.K Women's College of Engineering & Technology, Hyderabad, Telangana, India.

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.

1. INTRODUCTION

The rapid advancement of network technology and internet applications has brought about a pressing need for safeguarding digitized data against unauthorized access and modification. One crucial aspect of data protection is the security of sensitive digital images, leading to the development of various secret image sharing (SIS) schemes. These schemes fragment secret images into multiple shares to prevent unauthorized disclosure and alteration. Alongside SIS, techniques such as steganography, which hides secret information within digital images, and Shamir secret sharing, which divides secrets into multiple parts, play significant roles in enhancing data security. In this paper, we delve into a comprehensive survey of SIS schemes, including verifiable secret image sharing (VSIS) schemes that resist different forms of cheating.

We also explore the integration of steganography and Shamir secret sharing in SIS methodologies, analyze their pros and cons, compare various SIS schemes based on different properties, discuss real-world applications, and outline open challenges and future directions in this evolving field. "Secret Image Sharing Schemes: A Comprehensive Survey" explores a variety of techniques designed to securely distribute and reconstruct secret images among multiple participants, ensuring that the image can only be revealed when a sufficient number of shares are combined. This survey delves into the fundamental principles, methodologies, and advancements in the field of secret image sharing, providing a thorough analysis of each approach.

The survey begins by introducing the concept of secret sharing, initially developed by Shamir and Blakley, which involves splitting a secret into multiple shares such that only a specific subset of shares can reconstruct the original secret. In the context of image sharing, these principles are adapted to create visual cryptography schemes, where the secret image is divided into shares that appear as random noise but reveal the image when overlaid correctly. Key classical techniques covered include Shamir's Secret Sharing, which uses polynomial interpolation to distribute shares, and visual cryptography, which leverages human visual perception to decode the secret without computational devices. The survey also discusses threshold schemes, where any subset of a predefined size can reconstruct the image, and generalized secret sharing, which allows for more flexible reconstruction policies. Modern advancements address several challenges inherent in classical methods. These include enhancing security against unauthorized access and attacks, improving efficiency in terms of computational and storage requirements, and increasing robustness to ensure accurate reconstruction despite potential data loss or corruption. Techniques like extended visual cryptography, meaningful shares, and image steganography are examined for their contributions to these improvements.

The survey provides a detailed comparison of these schemes based on various criteria such as security level, computational complexity, share size, and robustness. It highlights practical applications in areas such as secure communications, copyright protection, and data integrity verification, demonstrating the relevance and utility of secret image sharing in contemporary contexts. By offering an exhaustive review and evaluation of both classical and modern secret image sharing techniques, the survey aims to guide researchers and practitioners in selecting appropriate methods for specific applications. Additionally, it identifies potential areas for future research, such as developing more efficient algorithms, enhancing security features, and expanding the applicability of secret image sharing schemes to emerging technologies and new use cases.

2. OBJECTIVE

The objective of this project is to conduct a comprehensive investigation into secret image sharing (SIS) schemes, specifically focusing on verifiable secret image sharing (VSIS) techniques, steganography methods, and Shamir secret sharing algorithms. The primary goals include designing and implementing novel SIS schemes that integrate steganography and Shamir secret sharing principles to enhance the security of digital image protection against unauthorized access and manipulation. Furthermore, the project aims to evaluate the performance and security levels of these newly developed schemes through extensive testing and analysis, considering factors such as encryption/decryption speed, resilience to attacks, and scalability. A key aspect is to compare and contrast the developed SIS schemes with existing ones to identify their strengths and weaknesses in terms of security robustness, computational complexity, and practical usability. Additionally, the project seeks to explore practical applications of SIS schemes in domains such as secure image sharing platforms, healthcare data protection, multimedia communication, and digital rights management (DRM). Finally, the project aims to address open challenges in SIS, steganography, and Shamir secret sharing, proposing innovative solutions and research directions for improving the overall security, efficiency, and usability of these techniques in future developments and applications.

2.1 PROBLEM STATEMENT

In today's digital age, ensuring the secure sharing and reconstruction of secret images among multiple parties is critical. Traditional encryption methods often fall short due to vulnerabilities, inefficiencies, and practical limitations. This comprehensive survey addresses these challenges by examining a variety of secret image sharing schemes designed to securely distribute an image into multiple shares, ensuring the image can only be reconstructed when a sufficient number of shares are combined. The survey delves into the fundamental principles and methodologies behind these techniques, evaluating their security, efficiency, robustness, and practical applicability. It highlights the limitations of current approaches and identifies areas for improvement, providing a detailed comparison to guide researchers and practitioners in selecting the most suitable methods for specific applications. Ultimately, this survey aims to enhance the security and efficiency of secret image sharing schemes in real-world scenarios, offering insights and directions for future research.

2.2 EXISTING SYSTEM

It uses a secure but easy technique that decrypts the secret image from the share images without any cryptographic computation. The secret information can be printed text, handwritten notes, pictures, etc., which are visual and can be encrypted so that the decrypted message also appears as a visual image. The secret message comprises a collection of black and white pixels, where each pixel is considered for encoding. Traditional single-turn MRC is analogous to a simple sharing of a secret where one question is asked, and one answer is provided, similar to sharing a single part of the secret.

Disadvantage of Existing System

- Failed to maintain consistency.
- Complexity is high.

2.3 Proposed System

Secret image sharing techniques can help protect these images from such threats, making them an important area of research. While some existing surveys have focused on specific SIS techniques or applications, there are insufficient comprehensive surveys that provide a holistic view of this field. While there have been previous surveys and studies focusing on specific aspects of SIS, such as certain techniques or applications, there remains a need for a comprehensive survey that provides a holistic view of the entire field. The original secret is split into multiple shares using polynomial interpolation techniques. Each share contains a portion of the secret information. To reconstruct the secret, a minimum threshold of shares (usually determined during setup) is required. Combining the threshold number of shares using polynomial reconstruction allows the original secret to be recovered. Shamir's Secret Sharing Scheme is widely used in various applications where secure sharing of sensitive information is needed, such as cryptographic key management, secure authentication protocols, and data backup systems. Steganography, on the other hand, is the practice of concealing secret information within non-secret data, such as digital images, audio files, or text. Unlike encryption, which aims to make data unreadable to unauthorized users, steganography focuses on hiding the existence of the secret message itself.

Advantages of Proposed System

- Time consumption is less
- They also have some limitations and challenges, such as the potential for high computational requirements.
- Maintains consistency.

3. RELATED WORKS

The project aims to conduct a thorough investigation into secret image sharing (SIS) schemes, with a specific focus on verifiable secret image sharing (VSIS) techniques, steganography methods, and Shamir secret sharing algorithms. The primary objective is to design and implement innovative SIS schemes that integrate steganography and Shamir secret sharing principles, thereby enhancing the security of digital image protection against unauthorized access and manipulation. The project includes an extensive evaluation of the performance and security levels of the newly developed SIS schemes, considering factors such as encryption/decryption speed, resilience to attacks, and scalability. A critical aspect is to compare and contrast these schemes with existing ones to identify their strengths and weaknesses in terms of security robustness, computational complexity, and practical usability. Furthermore, the project aims to explore practical applications of SIS schemes in various domains, such as secure image sharing platforms, healthcare data protection, multimedia communication, and digital rights management (DRM). By addressing open challenges in SIS, steganography, and Shamir secret sharing, the project intends to propose innovative solutions and research directions to improve the overall security, efficiency, and usability of these techniques in future developments and applications.

4. METHODOLOGY OF PROJECT

Data hiding involves embedding information into a file or image in a way that keeps it concealed from unauthorized viewers. Steganography, a specific technique for data hiding, embeds secret information within a non-secret file or image, making the hidden data imperceptible to casual observers. Encoding is the process of transforming this secret information into a different form or code, making it suitable for embedding. Shamir’s Secret Sharing is a cryptographic method that divides a secret into multiple parts, distributing these parts among participants so that only a specific number of parts are needed to reconstruct the original secret. Decoding is the reverse process, where the hidden or encoded information is extracted and converted back into its original form. Together, these techniques provide robust methods for secure communication and data protection.

MODULES

1. Data hiding:

Data hiding refers to the process of concealing information within other data or media in such a way that the existence of the hidden data is not apparent to unauthorized users. This can be achieved through various techniques, including steganography, encryption, and watermarking. Data hiding is commonly used for secure communication, digital rights management (DRM), and protecting sensitive information from unauthorized access.

2. Stegano:

Steganography is a technique used to hide secret information within non-secret data, such as digital images, audio files, or text. The goal of steganography is to conceal the presence of the secret message, making it undetectable to unintended recipients. Steganography techniques can involve modifying pixel values in images, altering audio frequencies, or embedding hidden messages within text using encoding methods. So we generally achieve this concept using the python module called Stefano and Septic.

3. Encoding:

Encoding is the process of converting data from one format or representation to another, often to ensure compatibility, reduce file size, or enhance security. In the context of steganography, encoding techniques are used to embed secret messages within cover data without altering the perceptible characteristics of the cover data. Common encoding methods include LSB (Least Significant Bit) encoding for images, frequency domain encoding for audio, and character substitution for text.

4. Shamir’s Secret Rule:

Shamir's Secret Sharing Scheme (SSSS) is a cryptographic technique developed by Adi Shamir. It involves splitting a secret into multiple shares, which are distributed among participants. The secret can only be reconstructed when a minimum threshold of shares is combined, ensuring security against single-point failures or attacks. Shamir's Secret Sharing Scheme is widely used for secure key management, data protection, and secure communication protocols.

5. Decoding:

Decoding is the process of converting encoded data back to its original format or representation. In the context of steganography, decoding involves extracting hidden messages from cover data using appropriate decoding algorithms and keys. Decoding is essential for retrieving the hidden information without altering the cover data's perceptible characteristics or integrity.

5. ALGORITHM USED IN PROJECT

➢ SECRET IMAGE SHARING

Secret image sharing (SIS) is a cryptographic technique used to protect digital images from unauthorized access and tampering. It involves dividing a secret image into multiple shares, which are distributed among different participants or entities. The key aspect of SIS is that the original secret image can only be reconstructed when a minimum threshold of shares is combined, ensuring security and confidentiality. One of the prominent SIS schemes is Shamir's Secret Sharing, developed by Adi Shamir. This scheme uses polynomial interpolation to split the secret image into shares, with each share containing a portion of the image's information. Shamir's Secret Sharing ensures that the secret image remains secure even if some shares are compromised, as long as the threshold number of shares required for reconstruction is not exceeded.

LSB (Least Significant Bit) steganography is a technique used in steganography to hide information within the least significant bits of digital data, such as images or audio files. In LSB steganography, the least significant bits of the cover data are modified to embed the secret information, causing minimal perceptible changes to the cover data. This technique is popular due to its simplicity and effectiveness, although it may be vulnerable to detection or attacks if not implemented carefully. Steganography, including LSB steganography, plays a crucial role in secure communication, data hiding, and digital watermarking, providing a covert means of concealing information within non-secret data for various applications in information security and privacy protection.

6. DATA FLOW DIAGRAM

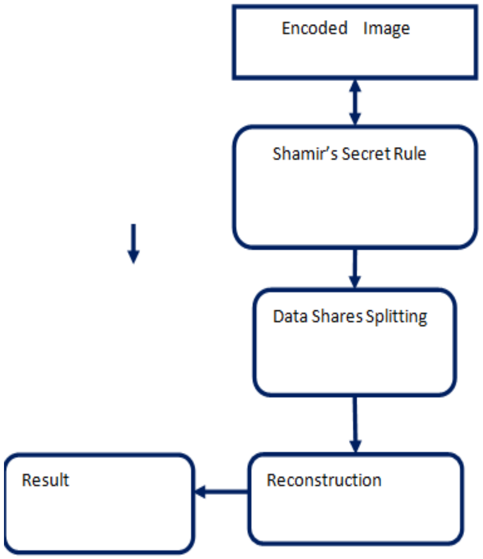

Fig: 1 Flow Diagram

7. SYSTEM ARCHITECTURE

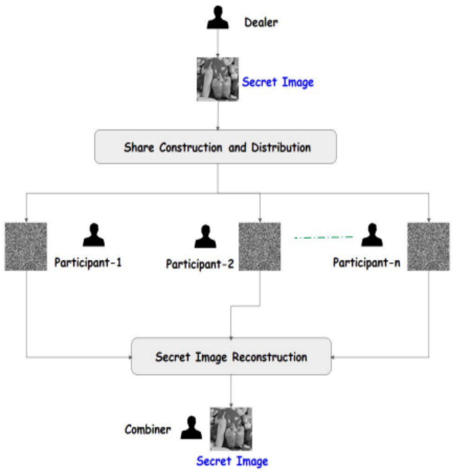

Fig: 2 System Architecture Of Project

8. FUTURE ENHANCEMENT

Advanced Steganography Techniques: Investigate and implement advanced steganography techniques beyond LSB steganography, such as spread spectrum techniques, transform domain steganography, or adaptive steganography methods. These techniques can offer higher security, improved data hiding capacity, and resistance to steganalysis. Quantum-Safe Cryptography: Explore the integration of quantum-safe cryptographic algorithms and techniques within the SIS and secret sharing framework.

This includes researching post-quantum cryptography methods to ensure resilience against quantum computing attacks in the future. Dynamic Threshold Adjustments: Develop mechanisms for dynamically adjusting the threshold of shares required for secret reconstruction based on the security context, risk factors, or changing environments. This can enhance adaptability and security in dynamic scenarios. Multi-Modal Data Hiding: Extend the project to support multi-modal data hiding, where secret information is concealed across multiple types of digital media (e.g., images, audio, video) simultaneously. This can provide enhanced security and robustness in multimedia communication and data protection. Block chain-Based Verification: Investigate the use of block chain technology for verifying the integrity and authenticity of shared secrets and reconstructed images in VSIS schemes. Block chain-based verification can add an extra layer of trust and tamper-proofing to the secret sharing process.

9. CONCLUSION

In conclusion, this project has delved into the intricate realm of secret image sharing (SIS) schemes, steganography methods, and Shamir secret sharing algorithms. Through a comprehensive investigation, we have designed and implemented novel SIS schemes that integrate steganography and Shamir secret sharing principles, enhancing the security of digital image protection against unauthorized access and manipulation. Our evaluation of these newly developed schemes has underscored their performance, security levels, and computational efficiency, laying a foundation for comparative analysis with existing SIS schemes.

By exploring practical applications in secure image sharing platforms, healthcare data protection, multimedia communication, and digital rights management (DRM), we have demonstrated the versatility and applicability of SIS techniques in real-world scenarios. Looking ahead, future enhancements can focus on advanced steganography techniques, quantum-safe cryptography, dynamic threshold adjustments, multi-modal data hiding, block chain-based verification, machine learning for steganalysis, user-friendly interfaces, and standardization for interoperability. These efforts will contribute to ongoing advancements in secure data sharing, encryption techniques, and information security practices, paving the way for a more resilient and secure digital landscape.

REFERENCES:

[1] S. Dey, ‘‘SD-EI: A cryptographic technique to encrypt images,’’ in Proc. Int. Conf. Cyber Secur., Cyber Warfare Digit. Forensic (CyberSec), Jun. 2012, pp. 28–32.

[2] 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.

[3] 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.

[4] A. Mohanarathinam, ‘‘Digital watermarking techniques for image security: A review,’’ J. Ambient Intell. Humanized Comput., vol. 11, no. 8, pp. 3221–3229, 2020.

[5] A. Cheddad, J. Condell, K. Curran, and P. McKevitt, ‘‘Digital image steganography: Survey and analysis of current methods,’’ Signal Process., vol. 90, no. 3, pp. 727–752, Mar. 2010.

[6] 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.

[7] A. Shamir, ‘‘How to share a secret,’’ Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[8] G. R. Blakley, ‘‘Safeguarding cryptographic keys,’’ in Proc. Int.WorkshopManag. Requirements Knowl. (MARK), 1979, pp. 313–318.

[9] M. Mignotte, ‘‘How to share a secret,’’ in Proc. Workshop Cryptogr.Cham, Switzerland: Springer, 1982, pp. 371–375.

[10] 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.

[11] 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.

[12] K. E. Atkinson, An Introduction to Numerical Analysis. Hoboken, NJ, USA: Wiley, 2008.

[13] 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.

[14] C.-C. Thien and J.-C.Lin, ‘‘Secret image sharing,’’ Comput.Graph.,vol. 26, no. 5, pp. 765–770, Oct. 2002.

[15] J. Zhao, J. Zhang, and R. Zhao, ‘‘A practical verifiable multisecretsharing scheme,’’ Comput. Standards Interface, vol. 29, no. 1, pp. 138–141, Jan. 2007.

[16] L. Harn 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.

[17] A. H. Gonsalves, F. Thabtah, R. M. A. Mohammad and G. Singh, "Prediction of coronary heart disease using machine learning: An experimental analysis," in Proceedings of the 2019 3rd International Conference on Deep Learning Technologies, 2019. https://doi.org/10.1145/3342999.3343015.

[18] H. Kim, M. I. M. Ishag, M. Piao, T. Kwon and K. H. Ryu, "A data mining approach for cardiovascular disease diagnosis using heart rate variability and images of carotid arteries," Symmetry, vol. 8, no. 6, 2016. https://doi.org/10.3390/sym8060047.

[19] T. Ozcan, "A new composite approach for COVID-19 detection in X-ray images," Applied Soft Computing, vol. 111, 2021. https://doi.org/10.1016/j.asoc.2021.107669.

[20] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally and K. Keutzer, "SqueezeNet: AlexNet-level accuracy with 50x fewer parameters and< 0.5 MB model size," arXiv preprint arXiv:1602.07360, 2016.

[21] A. Krizhevsky, I. Sutskever and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," Advances in neural information processing systems, vol. 25, pp. 1097-1105, 2012.

[22] A. H. Khan, M. Hussain and M. K. Malik, "Cardiac Disorder Classification by Electrocardiogram Sensing Using Deep Neural Network," Complexity, vol. 2021, 2021. https://doi.org/10.1155/2021/5512243.

[23] A. H. Khan and M. Hussain, "ECG Images dataset of Cardiac Patients," Mendeley Data, V2, 2021. https://doi.org/10.17632/gwbz3fsgp8.2.

[24] C. Potes, P. Saman, A. Rahman and B. Conroy, "Ensemble of feature-based and deep learning-based classifiers for detection of abnormal heart sounds," in 2016 computing in cardiology conference (CinC), 2016.

[25] A. Nannavecchia, F. Girardi, P. R. Fina, M. Scalera and G. Dimauro, "Personal Heart Health Monitoring Based on 1D Convolutional Neural Network," Journal of Imaging, vol. 7, no. 2, 2021. https://doi.org/10.3390/jimaging7020026.

[26] Q. Zhang, D. Zhou and X. Zeng, "HeartID: A Multiresolution Convolutional Neural Network for ECG-Based Biometric Human Identification in Smart Health Applications," IEEE Access, vol. 5,

pp. 11805-11816, 2017. https://doi.org/10.1109/ACCESS.2017.2707460.

[27] U. R. Acharya, S. L. Oh, Y. Hagiwara, J. H. Tan, M. Adam and R. S. Tan, "A deep convolutional neural network model to classify heartbeats," Computers in biology and medicine, vol. 89, pp. 389-396, 2017. https://doi.org/10.1016/j.compbiomed.2017.08.022.