TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

Privacy Protection Using Visual Secret Sharing Scheme: Review

Jasvant Kumar[1], Chandrajeet Yadav[2], and Hanuman Maurya[3]

[1]Department of Computer Science and Engineering, Faculty of Engineering and Technology, University of Lucknow, Lucknow, India
[2]Department of Computer Science and Engineering, Faculty of Engineering and Technology, Dr Shakuntla Misra National Rehabilitation University, Lucknow, India
[3]Department of Computer Science and Engineering Institute of f Engineering and Technology, Lucknow, India
er.jaswantsingh786@gmail.com[1] , chandrajeet86@gmail.com[2] , hanumanmaurya109@gmail.com

KEYWORDS

Privacy protection, security, image security, visual secret sharing, visual cryptography.

ABSTRACT

In the digital age, safeguarding sensitive visual data is a critical challenge due to its widespread use and the severe implications of unauthorized access. Visual Secret Sharing (VSS) schemes offer a robust solution by dividing a secret image into multiple, seemingly random shares that reveal no information individually. Only when a predefined number of shares are combined can the original image be reconstructed, ensuring privacy without reliance on complex computational decryption. Introduced by Naor and Shamir, VSS has evolved to support diverse applications, including secure document sharing, biometric authentication, and digital watermarking. This paper explores the principles, advancements, and practical implementations of VSS, highlighting its strengths—such as human-centric decryption and high security—and addressing limitations like pixel expansion and contrast loss. By examining its role in privacy protection across sectors like healthcare, finance, and e-voting, we demonstrate VSS's potential as a versatile tool for securing visual data in an interconnected world, while identifying future directions for enhancing its efficiency and scalability.

I. INTRODUCTION

In an era where digital data pervades every aspect of life, the protection of sensitive information has emerged as a critical concern across industries, governments, and individual users. Among the various forms of data, visual data—such as images, documents, and multimedia—poses unique challenges due to its widespread use and the severe consequences of unauthorized access. Images often contain sensitive information, such as medical records, financial documents, or proprietary designs, which, if compromised, can lead to significant privacy breaches, financial losses, or security threats. Traditional encryption methods, while effective for textual data, often require complex computational resources and decryption keys, which may not always be suitable for visual data or scenarios requiring human-verifiable security. The advent of Visual Secret Sharing (VSS) schemes offers a robust and innovative solution for enhancing the security of visual information.

VSS, a subset of visual cryptography, operates by decomposing a secret image into multiple, seemingly meaningless shares, which are then distributed among various participants. These shares, individually, reveal no information about the original image, ensuring that the secrecy of the data remains intact. Only when a

Corresponding Author: Dr. Jasvant Kumar, Department of Computer Science and Engineering, Faculty of Engineering and Technology, University of Lucknow, Lucknow, India.
Email: er.jaswantsingh786@gmail.com

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

predefined

number of shares are combined—either by stacking transparencies in traditional VSS or through computational reconstruction in advanced schemes—can the original image be recovered. This unique property makes VSS particularly appealing for applications where secure data sharing and human verification are paramount. This paper explores the fundamental concepts of VSS, its evolution since its inception, its practical implementations across various sectors, and its strengths and limitations. By examining these aspects, we aim to provide a comprehensive understanding of VSS's role in securing visual data in an increasingly interconnected and data-driven world.

II. PRINCIPLES OF VISUAL SECRET SHARING

The concept of VSS was first introduced by Moni Naor and Adi Shamir in their seminal 1994 paper [1], "Visual Cryptography," presented at EUROCRYPT '94. Building on Shamir's earlier work on secret sharing [2], which focused on distributing a secret among multiple parties, Naor and Shamir adapted the concept to visual data, creating a framework where the decryption process requires no computational effort beyond the human visual system. In their original scheme, a secret image is divided into n shares, such that any k or more shares (where $k \leq n$) can reconstruct the image when stacked, but fewer than k shares reveal no information about the secret. This is known as a (k, n)-threshold scheme.

The brilliance of Naor and Shamir's approach lies in its simplicity and security. Each share is a collection of black-and-white pixels arranged in a way that appears random or meaningless when viewed independently. When the required number of shares is superimposed, the human visual system can discern the original image due to the alignment of pixel patterns, without the need for cryptographic keys or computational devices. This human-centric decryption process makes VSS particularly suitable for scenarios where computational resources are limited or where human verification is preferred.

Definition and Mechanism

VSS is a cryptographic technique that encrypts a visual image into multiple shares. Each share is a random pattern of pixels that appears meaningless on its own. However, when a sufficient number of shares are overlaid or combined, the original image is revealed.

Types of VSS

1. **(k, n)-Threshold VSS**: **(k, n)-Threshold VSS[3,4]** is the most commonly used type of VSS, where a secret image is divided into 'n' shares, and a minimum of 'k' shares are required to reconstruct the image. The security of the scheme is derived from the threshold, ensuring that fewer than 'k' shares reveal no information about the original image.
2. **Color VSS**: Color visual secret sharing [5,16,17] extends the basic VSS to handle colored images. Unlike grayscale VSS, color VSS requires more complex encoding schemes to manage the additional information inherent in color images. Techniques such as halftoning or dithering are often employed to simulate continuous-tone colors with binary patterns, making it possible to apply VSS principles to color images effectively.
3. **Progressive VSS**: In progressive VSS[6,7.8], the image reconstruction process is gradual. As more shares are added, the quality of the revealed image improves progressively. This approach is beneficial in scenarios where partial information can be useful, and it provides a flexible balance between security and accessibility.
4. **Extended VSS (EVSS)**: EVSS[9,10] incorporates additional features such as authentication and verification. By embedding auxiliary information into the shares, EVSS can provide mechanisms to verify the authenticity of the shares and ensure that the reconstructed image has not been tampered with.
5. **Dynamic VSS**: Dynamic VSS schemes [11,12] allow for changes in the threshold or the number of shares after the initial distribution. This flexibility is advantageous in dy namic environments where the requirements for access control might change over time, enabling more adaptable security solutions.

III. EVOLUTION AND ADVANCEMENTS OF VSS

Since its introduction, VSS has undergone significant advancements to address modern security needs and expand its applicability. Early VSS schemes were limited to binary (black-and-white) images and suffered from

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

issues such as pixel expansion (where shares are larger than the original image) and reduced contrast in the reconstructed image. Over the years, researchers have proposed several enhancements to overcome these limitations:

1. **Support for Grayscale and Color Images**: Initial VSS schemes were restricted to binary images, but subsequent research extended the framework to grayscale and color images. For instance, Hou [13] proposed methods for applying VSS to color images by leveraging color decomposition techniques, enabling applications in more complex visual data scenarios, such as medical imaging and digital art protection.
2. **Reduction of Pixel Expansion**: Pixel expansion, where each pixel in the original image is represented by multiple sub-pixels in the shares, increases storage and transmission overhead. Yang [19] introduced probabilistic VSS schemes that minimize or eliminate pixel expansion, improving efficiency and practicality.
3. **Improved Contrast and Visual Quality**: Early VSS schemes often produced reconstructed images with poor contrast, making them difficult to interpret. Advances by Blundo et al.[14]focused on optimizing contrast in VSS, ensuring that reconstructed images are clearer and more usable.
4. **General Access Structures**: While Naor and Shamir's original work focused on threshold schemes, Ateniese et al. [15] extended VSS to general access structures, allowing more flexible rules for which combinations of participants can reconstruct the secret. This is particularly useful in hierarchical or role-based access control scenarios.
5. **Random Grid-Based VSS**: Shyu [18]introduced random grid-based VSS, which eliminates the need for pixel expansion and simplifies share generation, making it more practical for real-world applications.

These advancements have broadened the scope of VSS, enabling its use in diverse domains such as secure document sharing, biometric authentication, and digital watermarking.

IV. PRACTICAL IMPLICATINS OF VSS

1. **Secure Data Sharing:** VSS is widely used for secure data sharing in scenarios where sensitive information needs to be protected. By distributing shares among multiple parties, the security of the data is ensured as no single party can access the complete information. This application is especially relevant in environments where data integrity and confidentiality are paramount, such as financial institutions, healthcare, and government sectors.
2. **Authentication Systems:** VSS enhances security in authentication systems by requiring users to present multiple shares to gain access. This multi-factor authentication mechanism ensures that even if one share is compromised, unauthorized access is prevented. VSS-based authentication systems are used in high-security environments such as military installations, research labs, and secure online services.
3. **Copyright Protection:** By embedding copyright information into images using VSS, owners can protect their intellectual property. Only authorized individuals with the correct shares can access the protected content. This application is crucial in the digital media industry, where unauthorized distribution of copyrighted material is a significant concern. VSS ensures that only legitimate users can view or distribute the content, providing a robust deterrent against piracy.
4. **Secure Voting Systems:** VSS can be applied to secure electronic voting systems, ensuring the confidentiality and integrity of the voting process. Each voter's choice can be divided into shares, and only the combination of these shares can reveal the actual vote. This ensures that individual votes remain confidential, and the overall voting process is transparent and tamper-proof.
5. **Medical Image Security:** In the healthcare sector, VSS is used to protect sensitive medical images such as X-rays, MRIs, and CT scans. By dividing these images into shares and distributing them across different servers or stakeholders, patient privacy is maintained, and the risk of unauthorized access or data breaches is minimized.
6. **Cloud Storage Security:**With the increasing reliance on cloud storage, VSS provides a method for securing data stored in the cloud. By dividing files into shares and storing them across multiple cloud servers, the security and privacy of the data are enhanced. Even if one server is compromised, the data remains secure as long as the threshold number of shares is not reached.

V. STRENGTHS OF VISUAL SECRET SHARING

Visual Secret Sharing (VSS) is a cryptographic technique that distributes a secret image among multiple participants, where the secret can only be reconstructed by combining a sufficient number of shares. Here are the key strengths of VSS:

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

1. **No Computational Complexity for Decryption**: VSS relies on human visual perception to reconstruct the secret image by stacking shares (e.g., transparencies). No computational devices or complex algorithms are needed, making it simple and accessible.
2. **Perfect Secrecy**: Individual shares reveal no information about the secret image. Unless the required number of shares (threshold) is combined, the secret remains completely hidden, ensuring high security.
3. **Simplicity and Ease of Use**: The process of reconstructing the secret is intuitive—stacking physical or digital shares—making it user-friendly, even for non-technical users.
4. **Flexible Threshold Schemes**: VSS supports (k, n)-threshold schemes, where the secret can be reconstructed only when k out of n shares are combined. This flexibility allows customization based on security needs.
5. **No Need for Cryptographic Knowledge**: Unlike traditional encryption, VSS doesn't require users to understand cryptographic algorithms, as the reconstruction is purely visual.
6. **Robust Against Partial Attacks**: Since individual shares contain no usable information, an attacker with fewer than the required number of shares gains no advantage, enhancing security.
7. **Versatile Applications**: VSS is useful in scenarios like secure data storage, authentication systems, watermarking, and access control, especially in environments where computational resources are limited.
8. **Tamper Evidence**: Any alteration to a share is often visually detectable, making it difficult for malicious actors to manipulate shares without notice.
9. **Support for Various Image Types**: VSS can handle binary, grayscale, or even color images (with advanced schemes), making it adaptable to different use cases.
10. **Decentralized Trust**: By distributing shares among multiple parties, VSS eliminates the need for a single trusted authority, reducing the risk of a single point of failure.

These strengths make VSS particularly valuable in scenarios requiring secure, user-friendly, and computation-free secret sharing.

VI. LIMITATIONS OF VISUAL SECRET SHARING

While Visual Secret Sharing (VSS) has notable strengths, it also comes with several limitations:

1. **Pixel Expansion**: VSS often requires shares to be larger than the original secret image due to pixel expansion, increasing storage and transmission requirements.
2. **Loss of Image Quality**: Reconstructed images may suffer from reduced contrast or resolution, especially in basic VSS schemes, making fine details less clear.
3. **Limited to Visual Reconstruction**: VSS relies on human vision for decoding, which limits its use in automated systems or scenarios requiring digital processing.
4. **Physical Share Management**: If shares are physical (e.g., transparencies), they can be lost, damaged, or stolen, complicating secure storage and distribution.
5. **Threshold Constraints**: The (k, n)-threshold scheme requires exactly k shares to reconstruct the secret. If fewer than k shares are available, the secret cannot be recovered, which can be problematic in some scenarios.
6. **Complexity for Color Images**: Basic VSS schemes work best with binary images. Handling grayscale or color images requires more complex techniques, increasing computational overhead and share size.
7. **Alignment Issues**: When stacking physical shares (e.g., transparencies), precise alignment is needed to reconstruct the secret accurately, which can be challenging.

These limitations make VSS less suitable for certain applications, particularly those requiring high-resolution images, digital processing, or flexible recovery mechanisms.

VII. PRIVACY PROTECTION IN HEALTHCARE, FINANCE AND E-VOTING

Privacy protection is a critical concern across sectors handling sensitive personal data, especially in an era of increasing digitalization and cyber threats. As of September 2025, regulations emphasize consent, data minimization, security safeguards, and enforcement mechanisms, though challenges like cross-border data flows and emerging technologies persist. Below, I outline key protections in each sector, drawing on major frameworks and recent developments.

1.**Healthcare:** Healthcare involves highly sensitive protected health information (PHI), such as medical records and genetic data. Protections focus on restricting access, requiring consent for sharing, and mandating breach notifications.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

HIPAA Privacy and Security Rules (U.S.): The Health Insurance Portability and Accountability Act (HIPAA) safeguards PHI by limiting disclosures to treatment, payment, or operations unless patient authorization is obtained. Covered entities (e.g., hospitals, insurers) must implement administrative, physical, and technical safeguards. In 2025, updates include finalized stricter security requirements, such as written documentation of risk analyses and enhanced encryption for electronic PHI.

State and Global Laws: As of 2025, 19 U.S. states have comprehensive privacy laws treating health data as "sensitive," requiring opt-in consent for processing and prohibiting sales without explicit permission. Globally, the EU's GDPR mandates data protection impact assessments for health data processing, with fines up to 4% of global revenue for violations; California's CCPA similarly grants consumers rights to access, delete, and opt out of health data sales.

Emerging Trends: New state laws in places like Washington, D.C., and Oregon (effective 2025) restrict geofencing near sensitive locations (e.g., clinics) and lower thresholds for applicability (e.g., 25,000 consumers/year for data sellers). Focus areas include AI-driven diagnostics and telehealth, where anonymization techniques like differential privacy are recommended.

Challenges include non-HIPAA data (e.g., wellness apps) falling under general privacy laws, leading to fragmented compliance.

***2.*Finance:** Financial data, including transaction histories and credit scores, is protected through rules emphasizing transparency, consent for sharing, and secure data handling to prevent fraud and identity theft.

Gramm-Leach-Bliley Act (GLBA) and FinancialPrivacy Rule: U.S. financial institutions must provide annual privacy notices detailing data-sharing practices with affiliates and third parties, allowing customers to opt out of nonessential disclosures. The FTC enforces this, with 2025 updates expanding to digital banking apps.

CFPB Personal Financial Data Rights (PFDR) Rule: This 2025 rulemaking promotes "open banking" by requiring banks to share data (e.g., account balances) with authorized third parties via secure APIs, but only with consumer consent and revocation rights. It includes safeguards against data misuse, such as deletion requirements post-authorization. An Advance Notice of Proposed Rulemaking in August 2025 seeks input on enhancing privacy amid reconsideration efforts.

State-Level Expansions: Eight new state privacy laws took effect in 2025 (e.g., in Delaware and Iowa), mandating data protection assessments for high-risk processing like financial profiling. The FTC's updated Children's Online Privacy Protection Act (COPPA) now impacts youth financial products, requiring verifiable parental consent for data collection.

Key innovations include tokenization for masking sensitive data in transactions and biometric authentication with privacy-by-design principles.

***3.*E-Voting:**Electronic voting systems prioritize voter anonymity (the secret ballot) while ensuring verifiability and resistance to tampering. Privacy protections focus on decoupling voter identity from ballot choices, often through cryptographic methods, amid concerns over internet-based voting.

Voluntary Voting System Guidelines (VVSG 2.0): Issued by the U.S. Election Assistance Commission, these 2025 standards require voting systems to use end-to-end verifiability (e.g., paper trails) and prohibit internet connectivity to prevent remote hacks. Privacy features include voter-specific audit logs without revealing choices and accessibility for disabled voters without compromising anonymity.

Data Protection Compliance: Systems must adhere to GDPR-like rules for voter data (e.g., registration info), ensuring minimization (only essential data collected) and pseudonymization. In the EU, e-voting platforms require privacy impact assessments; U.S. states like Colorado use blockchain-inspired tech for secure, anonymous tallies.

Federal and Policy Measures: A March 2025 Executive Order emphasizes election integrity, mandating federal agencies to audit e-voting privacy risks and promote air-gapped systems (no internet). Organizations like EPIC advocate for protecting voter registration privacy against data brokers, including limits on sharing voter rolls.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

Internet voting remains insecure for widespread use due to vulnerabilities in email/mobile apps, with experts recommending hybrid systems (e.g., remote ballot marking with in-person delivery). Challenges include balancing accessibility with privacy in low-trust environments.

These frameworks evolve rapidly, with 2025 seeing heightened focus on AI and cross-sector data flows. For sector-specific compliance, consult legal experts.

VIII. CHALLENGES IN VSS

1. **Share Management:** Managing and securely distributing shares is a complex task. Ensuring that shares do not fall into unauthorized hands is crucial for maintaining the scheme's security. This involves not only secure transmission but also safe storage and access control mechanisms to prevent unauthorized retrieval or loss of shares.

2. **Image Quality:** The quality of the reconstructed image can vary significantly depending on the VSS scheme used. Balancing the trade-off between security and image quality is an ongoing research area. In many cases, achieving high security might lead to a reduction in the visual clarity of the reconstructed image, which can be a significant limitation for certain applications where image fidelity is crucial.

3. **Color and Grayscale Images:** Handling color and grayscale images in VSS requires more complex algorithms, which can increase computational requirements and complexity. Encoding color images often involves additional steps to manage the three color channels (RGB), leading to a more intricate share generation process. This complexity can pose challenges in terms of processing time and resource utilization, especially for high-resolution or large-scale images.

Sector	Key Regulations (2025)	Core Privacy Mechanisms	Enforcement/ Trends
Healthcare	HIPAA, GDPR, CCPA, 19 state laws	Consent for sharing, encryption, breach notifications	Stricter security docs; state opt-ins for sensitive data
Finance	GLBA, PFDR Rule, 8 new state laws, COPPA	Opt-out notices, API consent, data deletion rights	Open banking with revocation; youth data protections
E-Voting	VVSG 2.0, GDPR, Executive Order	Anonymization, no internet connectivity, verifiability	Air-gapped systems; audits for voter data brokers

4. **Scalability and Flexibility:** VSS schemes often face challenges related to scalability and flexibility. As the number of participants increases, managing and distributing a large number of shares can become cumbersome. Additionally, adapting the VSS scheme to different access structures or dynamic environments where the threshold might need to change poses significant technical challenges.
5. **Resistance to Collusion:** Ensuring that VSS schemes are resistant to collusion among participants is a critical challenge. If participants collude to gather shares without reaching the required threshold, they might attempt to reconstruct the secret image or infer sensitive information. Designing schemes that mitigate the risks of such collusion is essential for maintaining the integrity and security of the VSS system.
6. **Computational Overhead:** Although VSS is generally considered lightweight, certain types of VSS, particularly those dealing with color images or offering enhanced features like progressive reconstruction, can introduce significant computational overhead. This can be a limiting factor for real-time applications or systems with constrained computational resources.
7. **Real-Time Applications:** Improving the computational efficiency of VSS is essential for its application in real-time systems. Research efforts are focused on developing algorithms that can quickly generate and reconstruct shares, enabling VSS to be used in scenarios where rapid processing is critical. This includes areas such as live video streaming, real-time surveillance, and instant secure communication.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

8. **Quantum-Resistant VSS:** As quantum computing advances, traditional cryptographic methods face potential vulnerabilities. Developing quantum-resistant VSS schemes is a crucial future direction to ensure the long-term security of visual data. This involves exploring quantum-safe algorithms and integrating them with VSS to create robust solutions that can withstand the challenges posed by quantum computing advancements.

9. **User-Centric Designs:** Enhancing the usability of VSS for non-technical users is another important future direction. Developing intuitive interfaces, user-friendly share management tools, and simplified reconstruction processes will make VSS more accessible to a broader audience. This focus on user-centric designs aims to promote the widespread adoption of VSS in everyday applications, ensuring that privacy protection is available to all users regardless of their technical expertise.

IX. FUTURE DIRECTIONS

1. **Enhancing Image Quality:** Research is ongoing to improve the visual quality of reconstructed images in VSS. Techniques such as advanced pixel alignment, noise reduction algorithms, and machine learning models are being explored to enhance image clarity without compromising security. These innovations aim to make VSS more applicable in fields where high-quality visual output is critical, such as medical imaging and digital forensics.
2. **Expanding to Dynamic Environments:** Future VSS schemes are expected to be more adaptable to dynamic environments where user access levels and the number of participants can change frequently. Developing flexible threshold schemes and dynamic share allocation mechanisms will be crucial in making VSS more versatile and suitable for modern applications such as cloud computing and collaborative platforms.
3. **Integration with Emerging Technologies:** The integration of VSS with emerging technologies like blockchain, Internet of Things (IoT), and artificial intelligence (AI) is a promising area of research. By leveraging the decentralized and secure nature of blockchain, VSS can achieve enhanced security and traceability. Similarly, IoT devices can benefit from VSS to secure data transmission, while AI can optimize the share generation and reconstruction processes for better efficiency and accuracy.

X. CONCLUSION

Visual Secret Sharing (VSS) schemes have proven to be a critical advancement in the field of cryptography, offering a unique and effective means of securing visual information. By dividing a secret image into multiple, seemingly random shares, VSS ensures that sensitive information remains protected until the necessary threshold of shares is met for reconstruction. The diverse applications of VSS in areas such as secure data sharing, authentication systems, copyright protection, secure voting, medical image security, and cloud storage security highlight its versatility and importance in safeguarding visual data.

While VSS offers numerous advantages, including high security, minimal computational requirements, and robustness against data loss, it also faces challenges in areas like share management, image quality, and scalability. Addressing these challenges is essential for the continued evolution and effectiveness of VSS.

Looking ahead, the future of VSS is promising, with ongoing research aimed at enhancing image quality, adapting to dynamic environments, integrating with emerging technologies, and developing quantum-resistant schemes. By focusing on these future directions, VSS can continue to evolve and meet the growing demands for privacy protection in an increasingly interconnected and data-driven world. Through these advancements, VSS is set to play a pivotal role in securing visual data, ensuring that privacy and security remain paramount in the digital age.

References

[1] Naor, M., & Shamir, A. (1994). Visual Cryptography. *EUROCRYPT '94*, Springer, pp. 1-12. DOI: 10.1007/BFb0053414.

[2] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11), 612-613. https://doi.org/10.1145/359168.359176

[3] Liu, Zuquan, et al. "A novel (t, s, k, n)-threshold visual secret sharing scheme based on access structure partition." *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)* 16.4 (2020): 1-21.

[4] Kannojia, Suresh Prasad, and Jasvant Kumar. "XOR-based visual secret sharing scheme using pixel vectorization." *Multimedia Tools and Applications* 80.10 (2021): 14609-14635.

TEJAS Journal of Technologies and Humanitarian Science
ISSN-2583-5599
Vol.05, I.01 (2026)
https://www.tejasjournals.com/
https://doi.org/10.63920/ICFCSAI2025.009

[5] Yang, Ching-Nung, and Chi-Sung Laih. "New colored visual secret sharing schemes." *Designs, Codes and cryptography* 20.3 (2000): 325-336.
[6] Hou, Young-Chang, et al. "Block-based progressive visual secret sharing." *Information Sciences* 233 (2013): 290-304.
[7] Yan, Xuehu, and Yuliang Lu. "Progressive visual secret sharing for general access structure with multiple decryptions." *Multimedia Tools and Applications* 77.2 (2018): 2653-2672.
[8] Kannojia, Suresh Prasad, and Jasvant Kumar. "Plane-Wise Encryption Based Progressive Visual Cryptography for Gray Image." *International Conference on Communication, Networks and Computing*. Singapore: Springer Singapore, 2018.
[9] Kannojia, Suresh Prasad, and Jasvant Kumar. "XOR-based unexpanded meaningful visual secret sharing scheme." *International Journal of Security and Networks* 14.1 (2019): 1-9.
[10] Yang, Ching-Nung, and Tse-Shih Chen. "Extended visual secret sharing schemes: improving the shadow image quality." *International Journal of Pattern Recognition and Artificial Intelligence* 21.05 (2007): 879-898.
[11] Yuan, Jiangtao, and Lixiang Li. "A fully dynamic secret sharing scheme." *Information Sciences* 496 (2019): 42-52.
[12] Li, Fulin, et al. "A verifiable (k, n)-threshold dynamic quantum secret sharing scheme." *Quantum Information Processing* 21.7 (2022).
[13] Hou, Y. C. (2003). Visual Cryptography for Color Images. *Pattern Recognition*, 36(7), 1619-1629. DOI: 10.1016/S0031-3203(02)00249-2.
[14] Ateniese, G., Blundo, C., De Santis, A., & Stinson, D. R. (2001). Extended Capabilities for Visual Cryptography. *Theoretical Computer Science*, 250(1-2), 143-161. DOI: 10.1016/S0304-3975(00)00238-8.
[15] Ateniese, Giuseppe, et al. "Visual cryptography for general access structures." *Information and computation* 129.2 (1996): 86-106.
[16] Hou, Y. C. (2003). Visual Cryptography for Color Images. *Pattern Recognition*, 36(7), 1619-1629. DOI: 10.1016/S0031-3203(02)00249-2.
[17] Chiu, P. Y., & Hsueh, S. Y. (2009). A Visual Cryptography Scheme for Color Images Using Halftone Technology. *IEEE Transactions on Image Processing*, 16(1), 36-45. DOI: 10.1109/TIP.2006.884928.
[18] Shyu, S. J. (2007). Image Encryption by Random Grids. *Pattern Recognition*, 40(3), 1014-1031. DOI: 10.1016/j.patcog.2006.07.014.
[19] Yang, Ching-Nung, and Tse-Shih Chen. "Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion." *Pattern Recognition Letters* 26.2 (2005): 193-206.