The ISC Int'l Journal of Information Security
ISeCure

October 2025, Volume 17, Number 3 (pp. 1–9)
http://www.isecure-journal.org

Presented at the ISCISC'2025 in TEHRAN, Iran.

A Secure and Verifiable Secret Sharing Scheme Using Neural Steganography and Hash-Based Authentication **

Majid Farhadi Sangdehi [1,*], Zohre Karimi [2], and Mohammad Amin khorzani [3]
[1] *Department of Math and Computer Science, Damghan University, Damghan, Semnan, Iran*
[2] *School of Engineering, Damghan University, Damghan, Semnan, Iran*
[3] *Faculty of Mathematics and Computer Science, Damghan university, Damghan, Semnan, Iran*

ARTICLE INFO.

Keywords:
Shamir verifiable secret sharing, AES-GCM, Neural Steganography, Attention U-Net, Hash Authentication, Robustness

Type:

doi:

ABSTRACT

This study presents a resilient and efficient architecture for securely distributing secrets to the public across untrusted networks. The proposed method integrates Shamir's Verifiable Secret Sharing with AES-GCM encryption to provide strong confidentiality and authentication guarantees. Each share is reinforced with cryptographic hash-based signatures and imperceptibly embedded within cover images using a neural steganographic framework based on an Attention U-Net enhanced with transformer mechanisms and Squeeze-and-Excitation blocks, allowing the system to place data in visually insensitive regions adaptively. The training process leverages a joint perceptual and structural loss function, ensuring high visual fidelity while preserving critical image features for robust message recovery. Experimental evaluations demonstrate superior performance in Peak Signal-to-Noise Ratio and Structural Similarity Index Measure, and a minimal Bit Error Rate across various distortions, including noise, blurring, and JPEG compression. Compared to existing methods, the framework provides enhanced protection against fraudulent participants or dealers, eliminates reliance on secure private channels, and enables the reuse of system components, offering a comprehensive solution for safe, verifiable secret sharing.

1 Introduction

Information security and the protection of sensitive data are of paramount importance in the digital era. With the rapid advancement of emerging technologies and the exponential growth in data exchange across various platforms, the need for effective methods to preserve confidentiality and ensure the secure transmission of information has become increasingly critical. In this context, secret sharing schemes have emerged as an efficient approach to enhance security and improve fault tolerance in information systems [1, 2].

In such schemes, a secret is divided among multiple participants so that only predefined subsets can reconstruct and access the original secret. This mechanism significantly strengthens system security against

* Corresponding author.
**The ISCISC'2025 program committee effort is highly acknowledged for reviewing this paper.
Email addresses: farhadi@du.ac.ir, z.karimi@du.ac.ir, Mohammadaminkhorzani@gmail.com
ISSN: 2008-2045

threats such as insider attacks and unauthorised access [3].

On the other hand, image steganography, as an advanced technique for concealing data within digital images, enables the covert transmission of confidential messages with minimal impact on visual quality. The integration of secret-sharing techniques with image steganography can result in systems with enhanced security and greater resilience against various forms of attack [4, 5].

The proposed framework leverages adaptive neural embedding via the U-Net architecture, together with cryptographic hash functions, to ensure that each share is both securely embedded and independently verifiable. This combination provides a significant advantage by mitigating fraudulent behaviour from participants or dealers, enabling trustworthy secret reconstruction even under adversarial conditions. Unlike conventional static embedding approaches, which often fail to detect or prevent manipulation, integrating hash-guided verification enables each share to be authenticated independently, ensuring verifiable integrity throughout the reconstruction process.

Moreover, this hybrid strategy demonstrates clear practical advantages in diverse scenarios. Experimental evaluations show that the method maintains high visual fidelity, strong resistance to distortions such as noise, blurring, and JPEG compression, and robust protection against sophisticated statistical steganalysis. The adoption of this framework ensures that sensitive information remains secure and the system is resilient, providing both operational reliability and trustworthiness for secure digital communications. Overall, the proposed approach represents a robust, efficient, and transparent solution for secure secret sharing and verifiable message transmission in real-world and adversarial environments.

2 Related Work

2.1 Steganography-Based Secret Sharing

In recent secret sharing approaches, image steganography techniques are utilised to enhance security and conceal the shares. In this method, a trusted dealer divides a secret into n image shares and distributes them among n participants. Only a subset of participants, consisting of at least k authenticated members, can reconstruct the original secret by combining their respective shares.

The steganography-based secret sharing process typically consists of two main phases: the sharing phase and the reconstruction phase.

In the first phase, the original secret is transformed into n binary shares. These shares are then input into a cryptographic generator function (Gen) to produce image-based shares. For each share, the dealer also generates a binary authentication code. These codes are embedded within the image shares using steganographic methods. Finally, the n images share—each containing confidential data and an authentication code—are distributed among the participants.

In the reconstruction phase, participants receive their image shares and perform a data extraction (steganalysis) process to retrieve the embedded binary shares and authentication codes. Upon successful verification of the shares, any authorised group of at least k valid participants can collaboratively reconstruct the original secret. This structure not only enhances the security of data transmission and storage but also enables the detection and prevention of participant fraud [6].

2.2 Hash Function-Based Secret Sharing

In this type of secret-sharing scheme, a dealer distributes a set of secrets $h_1, h_2, \ldots, h_r$ among n participants $P_1, P_2, \ldots, P_n$ using cryptographic hash functions, so that only authorised subsets of participants can reconstruct the original secrets.

Setup Phase:

Assume the dealer intends to share r secrets $h_1, h_2, \ldots, h_r$ among n participants $P_1, P_2, \ldots, P_n$. The dealer randomly generates n shadows $s_1, s_2, \ldots, s_n$ and sends them securely to the participants via a secure channel. The dealer then identifies all authorized subsets and computes:

$$hv_i = H(M_{prtv,i}), \quad i = 1, 2, \ldots,$$

$$w, \quad c_{ij} = hv_i \oplus h_j, \quad i = 1, 2, \ldots, w, \quad j = 1, 2, \ldots, r$$

Reconstruction Phase:

When an authorized subset $P_1, P_2, \ldots, P_t$ which forms the smallest qualified group, comes together, they can calculate: $hv_i = H(M_{prti,i})$ and retrieve the corresponding values c_{ij} from a public bulletin board. Using these, they can reconstruct the original secrets $h_1, h_2, \ldots, h_r$ [7].

2.3 Hash Function-Based Image Steganography

Hash function-based image steganography is a secure data-hiding technique in which an encrypted message is embedded in a digital cover image by leveraging the inherent randomness and unpredictability of cryptographic hash functions. Unlike traditional methods that may follow fixed or easily traceable embedding patterns, this approach leverages the hash function's pseudo-random output to determine embedding positions, thereby enhancing both the security and imperceptibility of the stego-image.

The algorithm begins by splitting an encrypted message into smaller segments suitable for embedding. A hash function is then applied to each segment (or to a key-related input) to generate pseudo-random coordinates within the cover image. These coordinates indicate the locations where bits of the encrypted message will be inserted into the cover image's pixel values.

The final output is a stego-image that visually resembles the original cover image while securely containing the hidden encrypted data. This technique provides strong resistance against statistical attacks and steganalysis methods, making it highly suitable for applications where confidentiality and undetectability of communication are critical [8].

In the related work, three primary approaches have been examined, each with inherent limitations. First, steganographic secret-sharing methods, which, despite their data-hiding capabilities, lack integrated verification mechanisms and demonstrate inadequate resistance to data distortion and sophisticated attacks. Second, hash function-based schemes that, while leveraging cryptographic security and providing initial verification capabilities, remain vulnerable to statistical analyses and visual attacks due to the absence of a robust steganographic layer, failing to guarantee complete secret reconstruction. Third, hash-based steganographic approaches, although efficient at data concealment, are limited by the lack of secret-sharing mechanisms and advanced verification capabilities, leading to unreliable reconstruction and compromised integrity assurance.

Neural network-based steganography has become a prominent field, moving beyond traditional methods that rely on fixed embedding patterns. These deep learning approaches yield more robust, imperceptible steganographic systems. A typical architecture is the autoencoder, which uses a single neural network to embed a message into a cover image and another to extract it. More recent advancements include generative frameworks such as GANs and diffusion models [9, 10]. These models can produce stego-images with exceptionally high visual fidelity, making them nearly indistinguishable from the original cover image. Some methods utilise invertible networks for high-capacity image hiding, while others are based on denoising diffusion probabilistic models.

While many of these methods primarily focus on achieving high imperceptibility and visual quality, the proposed framework integrates three key components—verifiable threshold secret sharing, cryptographic hash functions, and neural network-based steganography—thereby not only enhancing security and reliability but also establishing significant resilience against distortions and sophisticated attacks, while ensuring a trustworthy and verifiable secret reconstruction process.

3 Proposed Method

In the proposed scheme, a multi-layered security framework is presented for the secure transmission of confidential data. It leverages the synergy of three core components: symmetric encryption, verifiable secret sharing, and neural network-based steganography. The system is designed to ensure confidentiality, integrity, and verifiability of messages in untrusted digital environments. The proposed process consists of the following stages:

3.1 Message Encryption

In the first step, the input message is encrypted using AES to ensure strong confidentiality. Galois/Counter Mode (GCM) is specifically chosen because it simultaneously provides both privacy and integrity verification in a single, efficient operation, unlike other AES modes (e.g., CBC or ECB) that require separate mechanisms for authentication or are vulnerable to pattern leakage. This ensures robust protection against eavesdropping and tampering. To enable verifiability at the receiver's end, a SHA-256 hash of the original message is also computed and stored separately, serving as a reference during recovery to confirm that the decrypted message has not been altered, thereby complementing the authentication provided by AES-GCM.

3.2 Verifiable Secret Sharing

At this stage, the encrypted message is divided into n shares using Shamir's threshold secret-sharing scheme, so that the message can be reconstructed with at least k shares. To increase trust and prevent fraud during reconstruction, a verifiable version is adopted in which each share is associated with a cryptographic commitment based on a collision-resistant hash function[11]. These commitments allow each share to be independently verified by the receiver without revealing private keys or additional information. This mechanism provides resistance to share-substitution attacks and data forgery.

3.3 Conversion of Shares to Binary Format

The textual shares produced during the secret-sharing phase are converted to binary strings. These binary data structures are suitable for embedding into a digital image and serve as the hidden message for the next stage.

3.4 Neural Network-Based Steganography

The resulting bitstreams, along with the cover image, are fed into a neural network encoder based on the Attention U-Net architecture with Squeeze-and-Excitation (SE) blocks [12]. The encoder-decoder design of U-Net preserves spatial information, which is crucial for precise embedding and accurate recovery of secret data. At the same time, the attention mechanism identifies image regions with lower visual sensitivity, and the SE blocks recalibrate feature maps to emphasise important details, ensuring that the embedded data does not compromise the cover image quality. Together, these components enable adaptive and reliable data embedding, maintaining high visual fidelity and robust recoverability, and outperforming simpler CNNs or standard U-Net models. The network is trained end-to-end, guaranteeing that the hidden data can be accurately extracted even under potential distortions, without perceptible degradation of the cover image.

3.5 Embedding Shares into the Cover Image

In this stage, the binary data resulting from the secret-sharing process is embedded as a bitstream within the cover image. This embedding is performed directly on the original image using a trained neural network, without generating a new image or causing perceptible visual changes. The output of this stage is the original cover image containing the hidden content, where the encrypted message and the shared secret shares are imperceptibly embedded. The attention mechanism in the Attention U-Net architecture adaptively selects the precise embedding locations to prevent noticeable visual distortions and to maintain steganographic security against advanced analysers. The use of the Attention U-Net architecture, leveraging adaptive attention modules and a multi-scale structure, enables targeted, imperceptible embedding of the shared secret data, thereby preserving the image's visual quality while significantly enhancing resistance to statistical analyses and machine-learning-based attacks.

3.6 Applying Artificial Attacks

To simulate real-world conditions and evaluate the system's resilience in untrusted environments, a set of common artificial attacks—such as Gaussian noise, Gaussian blur, JPEG compression, and salt-and-pepper noise—is applied to the stego-image. The purpose of this stage is to assess the scheme's robustness against unintended modifications and malicious attacks.

3.7 Performance Evaluation

Finally, the system's performance is quantitatively evaluated using rigorous metrics. For visual quality assessment, PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index) are used to assess image quality degradation and structural preservation, respectively. Additionally, to determine the accuracy of message reconstruction, the Bit Error Rate (BER) between the original and recovered message is computed. These evaluations are conducted iteratively after each attack and recovery phase to analyse the system's resilience under various scenarios comprehensively.

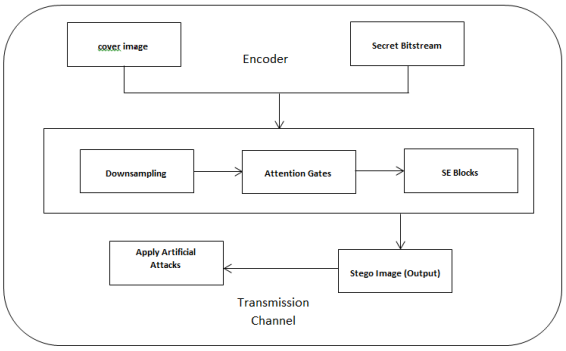


Figure 1. Steganographic Encoder / Sender Neural Network

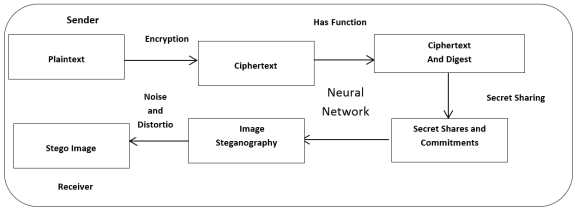


Figure 2. Share Generation Process

4 Secret Reconstruction Process

The secret reconstruction process is presented in Figure 2 It includes the following steps:

4.1 Receiving the Stego-Image

The receiver obtains the stego-image from the transmission channel. During transmission, the image may have been affected by various distortions, such as noise, blurring, or compression-induced artifacts.

4.2 Extraction of Hidden Data Using the Decoder Neural Network

The received image is passed through a decoder neural network. This decoder is architecturally symmetric and complementary to the encoder, and has been

jointly optimised during the training phase. Architectures such as Attention U-Net and SE blocks enhance the decoder's ability to accurately retrieve the hidden data, even under degraded image quality or adverse environmental conditions.

4.3 Reconstruction of the Encrypted Message via Verifiable Secret Sharing

The extracted bitstream is first converted into textual shares. Each share is then subjected to a verifiability check using cryptographic mechanisms such as hash functions, digital signatures, or other asymmetric authentication schemes. Only the shares that successfully pass the authenticity and integrity verification are used in the reconstruction process. Subsequently, Shamir's secret reconstruction algorithm with a predefined threshold is applied to recover the original encrypted message.

4.4 Decryption and Final Message Validation

The recovered encrypted message, previously encrypted with a symmetric algorithm (e.g., AES in GCM mode), is decrypted using the shared secret key. To ensure the integrity and authenticity of the message, the hash value computed from the decrypted message is compared with the original hash digest stored during the embedding phase. If the values match precisely, the message is confirmed as authentic and valid. Otherwise, it is flagged as tampered or invalid.

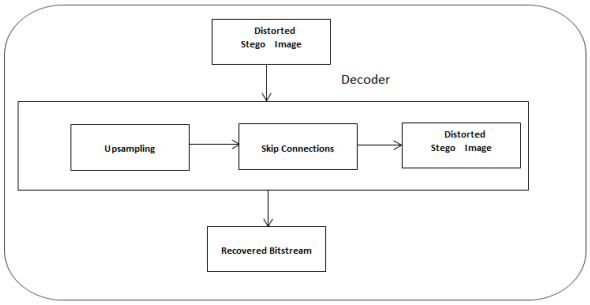


Figure 3. steganographic Decoder/Receiver Neural Network

5 Quantitative and Qualitative Evaluation

The model was trained on a randomly selected subset of 5,000 images from the Tiny-ImageNet dataset (original resolution $64 \times 64 \times 3$), normalized to the $[0, 1]$ range. The encoder architecture employed an Attention U-Net augmented with Squeeze-and-Excitation (SE) blocks (reduction ratio $r = 8$), while the decoder

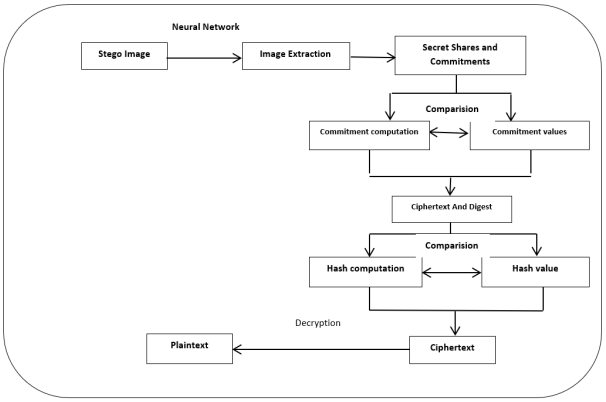
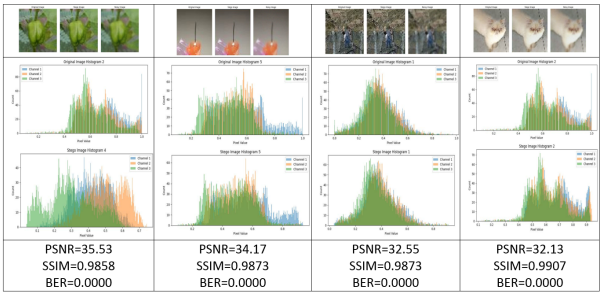


Figure 4. Secret Reconstruction Process

Table 1. Visual and Quantitative Analysis of Cover and Stego Images



comprised two convolutional layers with 64 and 128 filters, respectively. Training was conducted for 10 epochs with a batch size of 32, optimised using the Adam algorithm with learning rate $\eta = 10^{-3}$ and momentum parameters $\beta_1 = 0.9$ and $\beta_2 = 0.999$. A hybrid loss function was utilised, combining perceptual loss derived from the activations of the `block3_conv3` layer of a frozen VGG19 network (weighted by $\alpha = 0.6$) and SSIM loss (weighted by $\beta = 0.4$).

Table 1 presents the visual results of the steganographic system along with the corresponding quantitative evaluation metrics, including PSNR, SSIM, and BER. These metrics collectively assess the image reconstruction quality, structural similarity, and bit-level accuracy of the extracted secret. On average, the system achieved a PSNR of 31.21 ± 0.31 dB, an SSIM of 0.9961 ± 0.0043, and a BER of 0.0000 ± 0.0000, indicating that the generated stego-images are of high quality and visually imperceptible while remaining robust under practical distortion conditions.

The experiments were performed in a Google Colab environment equipped with a Tesla T4 GPU (16 GB VRAM) and 12 GB of system RAM. Training on the Tiny-ImageNet dataset took an average of 48 seconds per epoch, for a total of approximately 8 minutes over 10 epochs. The GPU memory usage peaked at around 9.5 GB.

Table 2 compares the proposed secret sharing scheme with other established methods from [6, 13–15] in terms of key security and performance features. The results indicate that the proposed scheme demonstrates higher resistance to participant and dealer fraud, enhances system reusability, and exhibits robustness against compression. Furthermore, the proposed approach does not require a private channel for shared transmission, thereby increasing efficiency and ease of implementation.

Table 2. Comparison Table of the Proposed Scheme with Other Methods

Feature	[6]	[13]	[14]	[15]	Proposed Scheme
Need for Private Channel	No	No	Yes	No	No
Resistance to Participant Fraud	No	No	Yes	No	Yes
Resistance to Dealer Fraud	Limited	No	Limited	No	Yes
Reusability of the System	Limited	Yes	Limited	Limited	Yes
Resistance to Compression	Vulnerable	Moderate	—	Weak	Yes

The proposed scheme exhibits a setup phase complexity of $O(e.b.f)$, reflecting a polynomial dependency on the number of participants, the size of data blocks, and the number of employed hash functions. This phase encompasses intricate operations involving secret sharing, cryptographic computations, and share preparation, leading to compounded computational overhead. The verification phase is modelled by a linear complexity of $O(f+n)$, representing the combined processing of hash functions and total shares, as share validation and data integrity checks necessitate parallel handling of these parameters. Finally, the reconstruction phase exhibits a complexity of $O(t2+n)$, where the quadratic term arises from Lagrange interpolation computations required to recover the secret from a minimum of t shares, and the linear term corresponds to the processing of all shares involved. This elevated computational complexity relative to simpler schemes is justified as a reasonable trade-off for ensuring the security, correctness, and robustness of the system.

Table 3. Comparison of Computational Complexity by Phase

Phase	[6]	[13]	[14]	[15]	Proposed Scheme
Setup	O(n)	O(n)	O(nlogn)	O(m)	O(e.b.f)
Verification	O(n)	O(??)	—	O(n)	O(f+n)
Reconstruction	O(n)	O(n)	O(nlogn)	O(n)	$O(t^2+n)$

6 Security Analysis of the Proposed Scheme

In this section, a comprehensive security analysis is presented for the hybrid system combining image steganography, secret sharing schemes, and a digital signature layer. The primary objective of this analysis is to evaluate the system's resilience against emerging threats and to assess the impact of integrating digital signatures on critical security properties such as confidentiality, data integrity, authentication, and non-repudiation [16, 17]. To enhance the security of the secret sharing scheme, three vital mechanisms are incorporated: share authentication, data integrity assurance, and non-repudiation.

6.1 Share Authentication

Each share generated within the (n, k) secret-sharing framework is cryptographically signed using public-key cryptography, such as EdDSA. This approach not only guarantees the authenticity of every share but also renders forgery or unauthorised share generation computationally infeasible without access to the private key [18, 19]. Consequently, this mechanism robustly protects the shares against attacks like forgery and impersonation.

6.2 Data Integrity Assurance

Before the secret reconstruction process, the validity and integrity of each share are verified by validating its digital signature with the corresponding public key. This mechanism detects even minimal modifications in the shared content, effectively preventing the use of tampered data. Therefore, only shares that remain unaltered and valid participate in the reconstruction of the secret [20, 21].

6.3 Non-Repudiation

The digital signature not only ensures authenticity and integrity but also enforces non-repudiation, meaning the sender cannot deny their involvement after a share is transmitted. This property is particularly crucial in legal contexts and sensitive information scenarios, enabling legal traceability in cases of misuse or malpractice [9, 22].

7 Conclusion

This research proposed a novel security framework for confidential data transmission that integrates three complementary technologies: image steganography, secret-sharing schemes, and neural networks. The system is designed to enhance data-hiding capacity, preserve the visual quality of the cover image, and ensure accurate recovery of embedded messages.

The integration of neural networks improves the efficiency of the embedding and extraction processes by enabling adaptive feature learning and robust optimization [23].

Empirical evaluations demonstrate that the proposed framework achieves high performance in terms of PSNR and SSIM metrics and shows strong robustness against statistical analysis and deep learning-based steganalytic attacks [10].

Furthermore, integrating a distributed secret-sharing architecture with enhanced cryptographic mechanisms at the steganography layer significantly strengthens the system's resistance to tampering, substitution, and reverse-engineering attacks [24].

Recent studies further confirm that the convergence of classical cryptography with modern deep learning architectures—especially autoencoder-based methods, invertible networks, and generative models such as diffusion models—provides a sustainable pathway for developing robust, high-quality data-hiding techniques [25, 26]. In this context, the proposed framework systematically combines verifiable secret sharing, cryptographic hash functions, and neural steganography, thereby ensuring accurate and verifiable recovery of embedded messages, maintaining the perceptual quality of cover images, and providing comprehensive protection against tampering, substitution, and statistical or learning-based attacks.

Future research will focus on enhancing the fidelity and security of steganographic techniques by integrating advanced generative frameworks, including diffusion models and invertible neural networks. In parallel, the development of quantum-resistant protocols for the secret-sharing component (post-quantum secret-sharing scheme) is essential to safeguard against emerging quantum threats. Furthermore, we can use post-quantum authentication for any share to satisfy post-quantum primitives [21], thereby strengthening the scheme's verifiability and resilience. Recognizing that the setup and reconstruction phases currently introduce higher computational costs—primarily due to cryptographic commitments, polynomial-based secret sharing, and interpolation—future work will explore algorithmic optimizations, precomputation strategies, and hardware acceleration to reduce latency and resource requirements. Designing lightweight, deployable neural architectures remains a priority for supporting resource-constrained and latency-sensitive environments, ensuring the practicality of the system. Additionally, large-scale empirical evaluations across heterogeneous network conditions will be conducted to rigorously validate the proposed framework's robustness, scalability, and real-world applicability.

References

[1] A. Beimel. Secret-sharing schemes: A survey. In *International Conference on Coding and Cryptology*, pages 11–46, Berlin, Heidelberg, 2011. Springer. URL https://doi.org/10.1007/978-3-642-20901-7_2.

[2] T. Tassa. Hierarchical threshold secret sharing. *Journal of Cryptology*, 20:237–264, 2007. URL https://doi.org/10.1007/s00145-006-0334-8.

[3] I. Alam, A. S. Alali, S. Ali, and M. S. M. Asri. A verifiable multi-secret sharing scheme for hierarchical access structure. *Axioms*, 13(8): 515, 2024. URL https://doi.org/10.3390/axioms13080515.

[4] A. Kaur, R. Kaur, and N. Kumar. A review on image steganography techniques. *International Journal of Computer Applications*, 123(4): 20–24, 2015. URL https://doi.org/10.5120/ijca2015905280.

[5] A. Gutub and M. Al-Ghamdi. Hiding shares by multimedia image steganography for optimized counting-based secret sharing. *Multimedia Tools and Applications*, 79(11):7951–7985, 2020. URL https://doi.org/10.1007/s11042-019-08427-x.

[6] K. Gao, Y. Wang, H. Li, and L. Zhang. Steganographic secret sharing via ai-generated photorealistic images. *EURASIP Journal on Wireless Communications and Networking*, 2022(1): Article 190, 2022. URL https://doi.org/10.1186/s13638-022-02190-8.

[7] M. Farhadi, H. Bypour, and R. Mortazavi. An efficient secret sharing-based storage system for cloud-based iots. In *2019 16th International ISC Conference on Information Security and Cryptology (ISCISC)*, pages 122–127, Mashhad, Iran, 2019. URL https://doi.org/10.1109/ISCISC48546.2019.8985146.

[8] Z. I. Nezami, H. Ali, M. Asif, H. Aljuaid, I. Hamid, and Z. Ali. An efficient and secure technique for image steganography using a hash function. *PeerJ Computer Science*, 8(2):e1157, 2022.

[9] J. Chen, H. Deng, H. Su, M. Yuan, and Y. Ren. Lattice-based threshold secret sharing scheme and its applications: A survey. *Electronics*, 13 (2):287, 2024. URL https://doi.org/10.3390/electronics13020287.

[10] H. Yang, Y. Xu, X. Liu, and X. Ma. Pris: Practical robust invertible network for image steganography. *arXiv*, 2023. URL https://doi.org/10.48550/arXiv.2309.13620.

[11] S. Atapoor, K. Baghery, D. Cozzo, and R. Pedersen. Vss from distributed zk proofs and appli-

cations. Technical Report 2023/992, Cryptology ePrint Archive, 2023. URL https://eprint.iacr.org/2023/992.

[12] P. Ji, Y. Zhang, and Z. Lv. Edge-guided dual-stream u-net for secure image steganography. *Applied Sciences*, 15(8):4413, 2025. URL https://doi.org/10.3390/app15084413.

[13] G. Li, S. Li, Z. Qian, and X. Zhang. Cover-separable fixed neural network steganography via deep generative models. In *Proceedings of the 32nd ACM International Conference on Multimedia*, pages 11719–11728, 2024.

[14] H. Zhou. Private neural network training with packed secret sharing. In Y. Chen, X. Gao, X. Sun, and A. Zhang, editors, *Computing and Combinatorics: COCOON 2024*, volume 15161 of *Lecture Notes in Computer Science*, pages 66–77. Springer, Singapore, 2025. URL https://doi.org/10.1007/978-981-96-1090-7_6.

[15] Z. Saeidi, A. Yazdi, S. Mashhadi, M. Hadian, and A. Gutub. High performance image steganography integrating iwt and hamming code within secret sharing. *IET Image Processing*, 18(1):129–139, 2024. URL https://doi.org/10.1049/ipr2.12938.

[16] C. C. Lin and W. H. Tsai. Secret image sharing with steganography and authentication. *Journal of Systems and Software*, 73(3):405–414, 2004.

[17] Z. Eslami, S. H. Razzaghi, and J. Z. Ahmadabadi. Secret image sharing based on cellular automata and steganography. *Pattern Recognition*, 43(1):397–404, 2010. URL https://doi.org/10.1016/j.patcog.2009.06.007.

[18] P. Singh and N. Sharma. Authentication and integrity verification in secret sharing schemes using lattice-based digital signatures. *IEEE Transactions on Dependable and Secure Computing*, 2023. URL https://doi.org/10.1109/TDSC.2023.3278491. Advance online publication.

[19] K. Woźniak, M. R. Ogiela, and L. Ogiela. A two-phase embedding approach for secure distributed steganography. *Sensors*, 25(5):1448, 2025. URL https://doi.org/10.3390/s25051448.

[20] V. Rajkumar, M. Prakash, and V. Vennila. Secure data sharing with confidentiality, integrity and access control in cloud environment. *Computer Systems Science & Engineering*, 40(2), 2022. URL https://doi.org/10.32604/CSSE.2022.019622.

[21] W. Shen, J. Qin, J. Yu, R. Hao, and J. Hu. Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage. *IEEE Transactions on Information Forensics and Security*, 14(2):331–346, 2018.

[22] L. Chen, D. Moody, A. Regenscheid, and A. Robinson. Digital signature standard (dss). Technical report, NIST, 2023.

[23] Z. Chen, T. Liu, J.-J. Huang, W. Zhao, X. Bi, and M. Wang. Invertible mosaic image hiding network for very large capacity image steganography. *arXiv*, 2023. URL https://doi.org/10.48550/arXiv.2309.08987.

[24] S. Sharma, S. Shivani, and N. Saxena. A self-authenticating multi-tone secret sharing scheme using meaningful shares for satellite images. *IEEE Access*, 2024.

[25] J. E. Nalavade, A. Patil, A. Buchade, and N. Jadhav. Deep neural network and gan-based reversible data hiding in encrypted images: A privacy-preserving approach. *SN Computer Science*, 5(1):45, 2023. URL https://doi.org/10.1007/s42979-023-02347-2.

[26] Y. Peng, Y. Wang, D. Hu, K. Chen, X. Rong, and W. Zhang. Stegaddpm: Generative image steganography based on denoising diffusion probabilistic model. In *Proceedings of the 32nd ACM International Conference on Multimedia*, pages 3001–3009, 2024. URL https://doi.org/10.1145/3581783.3612514.

Majid Farhadi Sangdehi is currently an Assistant Professor in the Department of math & Computer Science at Damghan University, Damghan, Iran. He received his Ph.D. in Coding Theory and Cryptography from Toulouse 2 university –Toulouse –France in 2007. Prior to that, he earned his M.Sc. degree in Computational Geometry from Amirkabir University of Technology in 2003, and his B.Sc. degree in mathematics from the Faculty of Math and Computer science at Amirkabir University of Technology in 2000. His research interests include cryptography, coding theory, secret sharing, IoT, computational algebraic geometry.

Zohre Karimi is currently an Assistant Professor in the Department of Computer Engineering at Damghan University, Damghan, Iran. She received her Ph.D. in Artificial Intelligence from Amirkabir University of Technology in 2018. Prior to that, she earned her M.Sc. degree in Software Engineering from Sharif University of Technology in 2010, and her B.Sc. degree in Software Engineering from the Faculty of Electrical and Computer Engineering at Shahid Beheshti University in 2006. Her research interests include machine learning, data mining, natural language processing, machine vision, and deep learning.

Mohammad Amin Khorzani is currently a Master's student in Cryptography and Coding at Damghan University, Damghan, Iran. He holds a B.Sc. degree in Mathematics Education from Ayatollah Khamenei Campus of Farhangian University, Gorgan, Iran. Alongside his graduate studies, he works as a mathematics teacher. His academic interests include cryptography, information security, secret sharing schemes, steganography, and neural network-based secure communication.