System For Covert Message Transmission Using Blockchain Platform for Steganography Images

Shreemathi.V[1], Venkatasubramanian Sivaprasatham[2], Dr. Magesh Kasthuri[3], Dr.S. Babu[4]
[1]*University of Technology and Applied Sciences, Oman*
[2]*University of Technology and Applied Sciences, Oman*
[3]*Chief Architect, Wipro Limited, India*
[4]*Assistant Professor, SCSVMV University, India*

***Abstract*—Steganography, the practice of concealing the existence of information within innocuous carriers, has gained renewed interest in an era where digital communication is ubiquitous and threats to privacy and information security are ever-present. Blockchain technology, with its decentralized, immutable, and transparent ledger, presents a novel platform for steganographic communication. Integrating steganography within blockchain systems aims to leverage blockchain's network and storage capabilities to transmit hidden messages in a manner that is both robust and resistant to tampering or detection.**

***Index Terms*—Blockchain, Steganography, covert, cryptography.**

I. INTRODUCTION

The intersection of steganography and blockchain technology offers a promising avenue for secure transmission of sensitive information. The novel approach lies in utilization of steganography for covert message transmission within blockchain frameworks such as OpenChain and Hyperledger. The paper explores detailed use case examples, particularly in the sharing of Electronic Medical Records (EMR) for patients, including high-profile individuals like members of royal families and statesmen, across hospitals and countries to prevent tampering or leaking of personal information.

II. LITERATURE REVIEW

The interplay of steganography and blockchain technology has piqued considerable academic interest, leading to an influx of research papers addressing the subject. A review of approximately 40 scholarly articles reveals a multitude of innovative approaches and applications, emphasizing the critical role of these technologies in securing data transmission.

This literature review synthesizes findings from approximately twenty research articles—selected from the provided references—exploring the system approaches and key metrics for developing blockchain-based steganographic systems. The following table organizes these studies according to author, publication year, system approach, and key metrics, followed by a critical discussion of prevailing trends, innovations, and challenges in the field.

Author(s) & Year	System Approach	Key Metrics / Outcomes
Torki et al. (2021)	High- and medium-capacity steganography algorithms using Bitcoin's address and transaction fields	Visibility, robustness, security, capacity; no manual data changes; practical limitations of prior schemes; up to 81.9 bits/transaction with 5 output addresses; challenges in detection and practical deployment
Zhang (2019)	DNA steganography combined with blockchain-based hash-chaining for physical object authentication	Key size (355 bits for author, 213 bits for third parties); labor-intensity of brute-force attacks; ability to evolve cryptographic and steganographic functions over time; cross-referencing for authenticity

Author(s) & Year	System Approach	Key Metrics / Outcomes
Chen et al. (2025)	Generic blockchain-based steganography framework (GBSF) with reversible GAN (R-GAN, CCR-GAN)	Channel capacity (up to 40 bits/field), concealment, scalability across Bitcoin/Ethereum fields; trade-off between capacity and concealment; theoretical justification for custom activation functions; outperforming prior state-of-the-art
Omego & Bosy (2025)	Hybrid steganographic model (cover modification + cover synthesis); multichannel protocol	Provable security against PPT adversaries; resilience to replay and man-in-the-middle attacks; adaptability for SMS banking/blockchain; security analysis via adversarial game model; improved undetectability and robustness
Szczypiorski & Tyl (2016)	Network packet timing steganography detection (MoveSteg)	Ability to trace source of timing-based steganography; limitations with multipath and node-induced delays; standard deviation and delay histogram as detection metrics
Xu et al. (2019; as reviewed by Torki et al., 2021)	Block transaction permutation by miner for data embedding	Impracticality due to need for mining power/pool control; minimal scalability; only pool managers can deploy; negligible applicability for general users

Author(s) & Year	System Approach	Key Metrics / Outcomes
Zhang et al. (2019; as reviewed by Torki et al., 2021)	Base58-encoded address generation and OP_RETURN embedding	Low capacity; reliance on OP_RETURN field raises suspicion; steganalysis feasible due to algorithmic predictability
Partala et al. (2019; as reviewed by Torki et al., 2021)	LSB embedding in transaction addresses (Bitcoin)	Extremely low throughput (1 byte/hour); sender/receiver coordination required; increased tracking risk; limited scalability
Rachmawanto & Sari (2017)	Image-based steganography with DCT and OTP encryption	Security enhancement via encryption; focus not on blockchain, but introduces metrics like imperceptibility and robustness applicable to blockchain-based schemes
El-Khamy et al. (2017)	Audio steganography using DWT and RSA encryption	Enhanced robustness and security; domain-specific, but evaluation metrics (robustness, capacity) parallel blockchain-based schemes
Mstafa & Elleithy (2016)	Video steganography using KLT tracking and error correcting codes	Emphasizes tracking and error correction for robust transmission; relevant for evaluating blockchain's inherent data integrity
Wang et al. (2022; as cited in Chen et al., 2025)	Required-field generation in blockchain via GANs	Concealment of covert channels by mimicking normal transaction field distributions;

Author(s) & Year	System Approach	Key Metrics / Outcomes
		challenges with embedding capacity and reversibility
Morkel et al. (2005)	General steganography overview (image focus)	Introduces four evaluation criteria: visibility, robustness, security, capacity; foundational metrics for blockchain-based schemes
Nakamoto (2008)	Bitcoin blockchain protocol	Provides the foundational infrastructure for blockchain-based steganography; key features include distributed consensus, permanence, and transaction field structures
Huh et al. (2017; as cited in Torki et al., 2021)	Blockchain for IoT device management	Not focused on steganography, but highlights the adaptability of blockchain for data transmission platforms
Zyskind et al. (2015; as cited in Torki et al., 2021)	Decentralized personal data management with blockchain	Demonstrates blockchain's suitability as a storage and transmission platform for sensitive data
Wang et al. (2019; as cited in Chen et al., 2025)	Deep generative models for field generation in blockchain	Use of GANs to generate indistinguishable required fields; addresses field redundancy and semantic challenges
Lin et al. (2017; as cited in Chen et al., 2025)	Deep learning for transaction field synthesis	Emphasizes model training and reversibility, influencing later reversible GAN approaches for steganography in blockchain
Zhang et al. (2018; as cited in Chen et al., 2025)	Statistical analysis for blockchain-based steganography detection	Evaluates detectability and provides benchmarks for concealment and capacity
Bosy & Omego (2024; as cited in Omego & Bosy, 2025)	Multichannel steganography protocol for SMS banking	Early multichannel protocol; identified vulnerabilities to replay and man-in-the-middle attacks; improved upon by later hybrid models

Challenges and Future Directions

The reviewed literature illustrates a progression from simplistic, low-capacity schemes to advanced, hybridized, and AI-enabled systems. Early blockchain-based steganography focused on modifying transaction addresses (e.g., LSB embedding, base58 address manipulation) or leveraging seldom-used fields (e.g., OP_RETURN) (Torki et al., 2021). However, these methods suffered from low throughput, high detectability, and impractical operational requirements—such as needing miner privileges or precise sender-receiver coordination.

Recent advances, such as the Generic Blockchain-based Steganography Framework (GBSF) proposed by Chen et al. (2025), leverage deep learning and generative adversarial networks (GANs) to synthesize required transaction fields. These approaches allow for increased channel capacity and improved concealment by producing transaction data that closely mimics legitimate blockchain activity. Reversible GAN architectures (R-GAN and CCR-GAN) further enable the recovery of embedded covert data, overcoming the traditional challenge of irreversibility in deep learning models.

Hybrid models, as discussed by Omego and Bosy (2025), combine cover modification and cover synthesis principles while employing multichannel protocols. This synthesis not only enhances undetectability but also provides resilience against advanced adversarial threats—including replay and man-in-the-middle attacks—by distributing secret data across multiple communication channels and employing integrity checks.

Beyond purely digital approaches, Zhang (2019) introduced a tangible dimension by embedding DNA-based steganographic keys within a blockchain signature chain, enabling authentication of physical objects. The time-stamped, hash-chained record structure allows for evolving cryptographic and steganographic mechanisms, further enhancing security over time.

Methodology

This research employs a qualitative approach to analyze the integration of steganography with blockchain technology. By examining various blockchain frameworks like OpenChain and Hyperledger, the study evaluates their compatibility with steganographic methods for data concealment and transmission. The research also involves case studies on the sharing of EMRs among hospitals and across countries, focusing on high-profile individuals.

Use Case Examples

Sharing Electronic Medical Records (EMR)

One of the critical applications of steganography with blockchain technology is in the secure sharing of Electronic Medical Records (EMR). Hospitals often need to share patient records for consultations, diagnoses, and treatment planning, which necessitates stringent measures to protect patients' privacy.

High-Profile Patients

When it comes to high-profile patients, such as members of royal families or statesmen, the stakes are even higher. The possibility of tampering or leaking sensitive information can have severe consequences. Steganography embedded within blockchain frameworks can significantly mitigate these risks. For instance, a hospital can encode a patient's EMR within a non-secret image or text, which is then transmitted through a blockchain network like OpenChain. The decentralized nature of blockchain ensures that the data remains tamper-proof and traceable, while steganography keeps the content hidden from unauthorized access.

Discussion

Steganography with blockchain technology offers a dual layer of security—steganography hides the existence of the message, while blockchain secures the transmission and maintains data integrity. This combination is particularly beneficial in the healthcare sector, where patient confidentiality is paramount. By using blockchain frameworks such as OpenChain or Hyperledger, hospitals can securely share EMRs without the fear of data breaches or tampering.

Advantages

- Enhanced Privacy: Steganography ensures that the message is concealed, making unauthorized access extremely difficult.
- Data Integrity: Blockchain technology guarantees immutability, preventing any alterations to the data.
- Traceability: Blockchain provides a transparent and traceable path for data transmission, ensuring accountability.
- Scalability: Blockchain frameworks can handle large volumes of data, making them suitable for extensive medical record sharing.

Conclusion

The integration of steganography and blockchain technology has evolved from rudimentary, low-capacity schemes to sophisticated, scalable, and secure systems leveraging AI, hybrid protocols, and even biological encoding. Key advances include the use of reversible deep learning models for field generation, hybrid cover strategies for enhanced security, and formal adversarial models to quantify protocol robustness. Despite these innovations, challenges remain—particularly in balancing capacity and concealment, ensuring scalability, and keeping pace with advancing detection techniques. Future research will likely focus on adaptive, context-aware steganographic systems capable of dynamically optimizing embedding strategies in response to evolving adversarial tactics and network conditions.

REFERENCES

[1] Chen, Z., He, J., Wang, J., Xiong, Z., Xiang, T., Zhu, L., & Niyato, D. (2025). Efficient Blockchain-based Steganography via Backcalculating Generative Adversarial Network. http://arxiv.org/pdf/2506.16023v1

[2] El-Khamy, S. E., Korany, N. O., & El-Sherif, M. H. (2017). A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform

domain and RSA encryption. Multimedia Tools and Applications, 76(22), 24091–24106.

[3] Morkel, T., Eloff, J. H., & Olivier, M. S. (2005). An overview of image steganography. ISSA, 1.

[4] Mstafa, R. J., & Elleithy, K. M. (2016). A video steganography algorithm based on Kanade-Lucas-Tomasi tracking algorithm and error correcting codes. Multimedia Tools and Applications, 75(17), 10311–10333.

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf

[6] Omego, O., & Bosy, M. (2025). Multichannel Steganography: A Provably Secure Hybrid Steganographic Model for Secure Communication. http://arxiv.org/pdf/2501.04511v1

[7] Rachmawanto, E. H., & Sari, C. A. (2017). Secure image steganography algorithm based on DCT with OTP encryption. Journal of Applied Intelligent System, 2(1), 1–11.

[8] Szczypiorski, K., & Tyl, T. (2016). MoveSteg: A Method of Network Steganography Detection. http://arxiv.org/pdf/1610.01955v1

[9] Torki, O., Ashouri-Talouki, M., & Mahdavi, M. (2021). Blockchain for steganography: advantages, new algorithms and open challenges. http://arxiv.org/pdf/2101.03103v1

[10] Zhang, Y. (2019). Blockchain of Signature Material Combining Cryptographic Hash Function and DNA Steganography. http://arxiv.org/pdf/1909.07914v1