Tuijin Jishu/Journal of Propulsion Technology
ISSN: 1001-4055
Vol. 46 No. 3 (2025)

Developing a Blockchain-Based System for Covert Steganographic Communication

Shreemathi.V[1], Dr.S.Babu[2], Dr.Magesh Kasthuri[3], Venkatasubramanian Sivaprasatham[4]

[1] *University of Technology and Applied Sciences, Oman*

[2] *Assistant Professor, SCSVMV University, India*

[3] *Chief Architect, Wipro Limited, India*

[4] *University of Technology and Applied Sciences, Oman*

Abstract:- In the digital age, the relentless advancement of communication technologies has brought forth both unprecedented opportunities and new challenges in data security. While cryptography has long served as the cornerstone for protecting the confidentiality of information, its presence alone can be a signal that sensitive data is being exchanged, thus potentially inviting scrutiny or attack. Steganography, in contrast, aims to conceal not only the content of a message but also the very existence of communication, offering a deeper layer of security by embedding covert messages within innocuous-looking carriers.

Keywords*: Blockchain, cryptography, steganography, EMR, government, e-governance.*

1. Introduction

With the emergence of blockchain technology—a decentralized, immutable, and transparent ledger system—new horizons for secure and covert communication have been unveiled. Blockchain's inherent features such as distributed consensus, global accessibility, and tamper-resilience make it an attractive platform for steganographic applications. The fusion of blockchain with steganography promises to revolutionize the way sensitive data, such as medical records or confidential government documents, is transmitted and stored without arousing suspicion.

This research paper explores the development of a blockchain-based system designed to transmit covert steganographic messages. The discussion encompasses a comprehensive literature review, a detailed description of the proposed system, its architectural design, and pertinent use cases, including medical record handling and the exchange of sensitive government information. We conclude by evaluating the strengths, limitations, and future challenges of leveraging blockchain for steganography.

2. Literature Review

Steganography: Principles and Evolution

Steganography, derived from the Greek words "steganos" (covered) and "graphein" (writing), is the art and science of hiding information within innocuous media such as images, audio, video, or even network protocols (Torki et al. 1). Its core objective is to ensure that the presence of a hidden message is undetectable to unintended observers. Traditionally, redundancy in media such as digital images or videos has facilitated the embedding of secret data without noticeable alterations. The success of steganography depends on several criteria: invisibility (imperceptibility of the steganogram), robustness (resilience to manipulations), security (difficulty of detection), and capacity (amount of data that can be hidden) (Torki et al. 5).

As steganalysis—the practice of detecting hidden messages—has advanced, so too have steganographic techniques. Early methods relied on modifying the least significant bits (LSB) of images or audio files, but these

techniques became susceptible to statistical attacks. Modern steganography often integrates cryptographic principles or leverages machine learning to generate or select cover media, enhancing both security and undetectability (Omego and Bosy 1).

Blockchain as a Platform for Steganography

Blockchain technology, initially popularized by Bitcoin, is a distributed ledger system maintained by consensus across a peer-to-peer network. Its key features include decentralization, transparency, immutability, and accessibility (Torki et al. 1). Every transaction recorded on a blockchain is time-stamped, cryptographically signed, and, once validated, becomes a permanent part of the ledger.

The readiness of blockchain as a data transmission and storage platform provides distinct advantages for steganography (Torki et al. 2). Unlike traditional media, where embedding secret data requires manual alteration of the carrier (and thus carries the risk of detection), blockchain allows for the generation of transaction fields that can inherently encode covert information without manual tampering. For example, by exploiting the randomness and flexibility in generating transaction addresses or amounts, one can embed hidden messages that are statistically indistinguishable from legitimate transactions.

Moreover, the frequent and routine nature of blockchain transactions reduces suspicion, as the transmission of data via blockchain is a common and expected activity. The global accessibility and persistence of the blockchain ledger further enhance its suitability for covert communication.

Advances in Blockchain-Based Steganography

Recent research has recognized the potential of blockchain as a steganographic carrier and introduced innovative algorithms to leverage its unique features. Torki et al. proposed two algorithms: a high-capacity embedding algorithm for exchanging keys and steganography parameters, and a medium-capacity algorithm for embedding the actual covert data (Torki et al. 4-5). These methods utilize Hierarchical Deterministic Wallets (HDW) to generate a vast array of addresses algorithmically, allowing for the selection of addresses or permutations that correspond to specific hidden data bits, all without altering the underlying blockchain data.

Other researchers have explored the use of generative adversarial networks (GANs) to synthesize blockchain transaction fields that encode covert messages. Chen et al. introduced a generic blockchain-based steganography framework (GBSF), featuring a reversible GAN (R-GAN) that can generate transaction fields (such as amounts or fees) embedding covert data. The receiver can then invert the generator to recover the hidden message. Enhancements such as counter-intuitive data preprocessing and custom activation functions have improved both the capacity and concealment of these schemes, enabling up to 40 bits of covert data per transaction field on standard blockchains (Chen et al. 1-3).

In the realm of hybrid steganographic models, Omego and Bosy combined cover modification and cover synthesis principles to create multichannel protocols adaptable to resource-rich environments like blockchain. Their approach increases resilience to advanced attacks and provides practical frameworks for secure steganographic communication in both constrained and high-bandwidth settings (Omego and Bosy 1).

Open Challenges and Limitations

Despite significant progress, several open challenges remain. As Torki et al. observed, developing algorithms that can embed high-capacity covert data in blockchain fields without manual changes is an ongoing endeavor. Moreover, designing steganalysis techniques that can reliably detect such embeddings is particularly difficult, given the indistinguishability of generated fields from genuine ones (Torki et al. 7).

Other challenges include the computational cost and scalability of advanced embedding schemes, the potential for detection if adversaries learn the specifics of the embedding algorithm, and the trade-off between channel capacity and concealment (Chen et al. 3-4). Furthermore, ensuring the long-term security and adaptability of steganographic schemes in the face of evolving analytical methods and regulatory scrutiny remains an active area of research.

3. Proposed System

Objectives and Design Rationale

The proposed system seeks to develop a robust, secure, and flexible framework for transmitting covert messages using blockchain as the carrier medium. The main objectives are:

1. **Covert Data Transmission:** Hide the very existence of secret communication by embedding messages within blockchain transactions, making detection by adversaries highly improbable.
2. **Security and Robustness:** Ensure that hidden data cannot be easily extracted or corrupted, leveraging blockchain's immutability and consensus protocols.
3. **Scalability and Adaptability:** Support a range of use cases, from low-capacity signaling to high-capacity data exchange, and adapt to different blockchains and transaction types.
4. **Undetectability:** Generate transaction fields that are statistically and functionally indistinguishable from normal blockchain activity.

To achieve these goals, the system integrates advanced steganographic algorithms with blockchain transaction generation, leveraging both deterministic and generative approaches to field creation.

System Overview

The core idea is to use blockchain transactions—not just as a record of value exchange, but as a covert communication channel. By algorithmically generating transaction fields (such as addresses, amounts, or scripts) that encode bits of secret data, the sender embeds the covert message directly in the transaction creation process. The receiver, with knowledge of the embedding algorithm and necessary keys, can retrieve the hidden information from the blockchain.

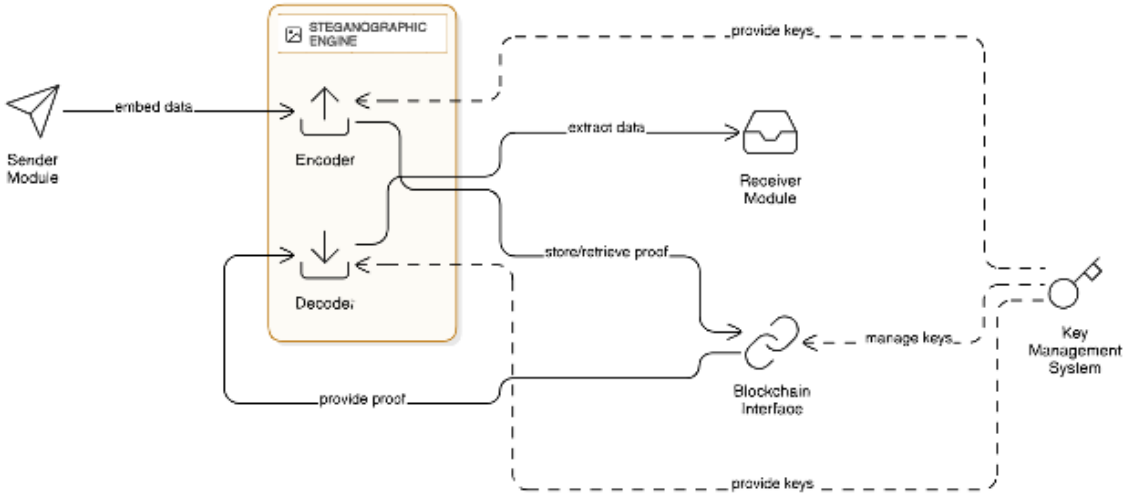

Figure 1: Component architecture of proposed system

The system supports two primary embedding modes:

- **High-Capacity Embedding:** Used for key exchange, steganography parameter agreement, and other operations requiring large payloads. This mode may incur the loss of transaction value (e.g., burned coins) but offers a larger embedding space (Torki et al. 4).
- **Medium-Capacity Embedding:** Designed for regular data transmission, this mode embeds smaller payloads per transaction but preserves transaction value, making it more suitable for ongoing covert communication (Torki et al. 5).

Advanced schemes may employ reversible GANs to synthesize transaction fields, further increasing capacity and concealment (Chen et al. 2).

4. Architecture of the Proposed System

System Components

The proposed architecture consists of the following components:

1. **Sender Module:** Responsible for encoding the covert message, generating the appropriate blockchain transaction fields, and broadcasting the transaction to the blockchain network.
2. **Receiver Module:** Monitors the blockchain for relevant transactions, decodes the covert message using the agreed-upon algorithm and keys, and reconstructs the original data.
3. **Key Management System:** Facilitates secure distribution and rotation of cryptographic keys required for embedding and decoding messages.
4. **Steganographic Engine:** Implements the embedding algorithms, including HDW-based address generation, field permutation, and GAN-based field synthesis.
5. **Blockchain Interface:** Connects to the blockchain network, enabling the creation, broadcasting, retrieval, and verification of transactions.

Workflow

1. Initialization and Key Exchange

Prior to communication, the sender and receiver agree on cryptographic keys and steganography parameters. This can be accomplished using the high-capacity embedding mode, where key material is encrypted and embedded into specially crafted transactions (Torki et al. 4).

2. Message Encoding

The sender divides the secret message into payload chunks suitable for embedding. For each chunk:

- The desired bits are mapped to transaction field values (e.g., specific addresses or amounts).
- Using the HDW algorithm, the sender iteratively generates candidate addresses or fields until one matches the desired bit pattern.
- For increased capacity, the sender may also permute the order of multiple output addresses, each permutation representing additional bits (Torki et al. 5).
- Alternatively, the sender may use a reversible GAN to synthesize transaction fields, embedding covert data directly in the generator's input noise (Chen et al. 2).

3. Transaction Creation and Broadcast

The sender constructs the final transaction, incorporating the generated fields, and broadcasts it to the blockchain network as a standard transaction.

4. Message Decoding

The receiver, monitoring the blockchain, identifies relevant transactions (e.g., by matching input addresses generated via HDW or by following a predetermined schedule). Using the shared keys and embedding algorithm, the receiver reconstructs the original message by extracting bits from transaction fields and their permutations.

5. Key Update and Session Management

For prolonged communication, the sender and receiver can periodically update their keys using the high-capacity embedding mode, ensuring ongoing security.

Security and Performance Considerations

- **Visibility:** The embedding process does not manually alter existing blockchain data; instead, it selects or generates fields that naturally encode the desired bits, maintaining the indistinguishability of covert transactions (Torki et al. 5).
- **Robustness:** Data is preserved by the blockchain's consensus protocol and digital signatures, ensuring it cannot be tampered with or lost (Torki et al. 5).
- **Security:** Without knowledge of the embedding algorithm and keys, adversaries cannot distinguish covert transactions from regular activity (Torki et al. 5; Chen et al. 3).
- **Capacity:** The maximum data embedded per transaction depends on the chosen algorithm, the number of output addresses, and the permissible field range. GAN-based approaches can reach up to 40 bits per field, while HDW-based methods scale with the number of address permutations (Chen et al. 3; Torki et al. 5).

5. Use Cases

Medical Record Handling Using Blockchain and Steganography

The management of medical records involves a delicate balance between accessibility, privacy, and integrity. Unauthorized access to patient data can have severe legal and ethical consequences, while loss or tampering of records can endanger patient safety. Blockchain, with its immutable ledger and distributed architecture, offers a promising foundation for secure healthcare data management. However, conventional blockchain-based systems, while transparent and tamper-resistant, might expose metadata or transaction patterns that could be exploited to infer sensitive information.

By integrating steganography into blockchain-based medical record systems, healthcare providers can achieve an additional layer of privacy. For example, a hospital could embed patient identifiers or sensitive metadata within the structure of blockchain transactions, such as in the generation of output addresses or transaction amounts, rather than storing them as explicit data fields. Steganographic embedding ensures that the presence of sensitive information is concealed even from entities monitoring blockchain activity.

In practice, when a new medical event (such as a diagnosis or prescription) is recorded, the relevant information is encoded using the system's steganographic engine and embedded in a dedicated blockchain transaction. Only authorized parties with the correct keys and algorithms can decode and interpret the data, while others see only routine transactional activity. This approach not only protects patient privacy but also leverages the blockchain's auditability and data integrity features (Omego and Bosy 1).

Moreover, the system's adaptability allows it to scale across institutional boundaries, supporting secure inter-hospital communication, insurance claims, and regulatory reporting, all while maintaining the covert nature of sensitive exchanges.

Government Secret Document Sharing via Blockchain and Steganography

Government agencies, law enforcement, and military organizations routinely exchange confidential reports, intelligence data, and sensitive operational information. The exposure of such documents can have far-reaching national security implications. Traditional secure communication channels—reliant on encryption—can be susceptible to interception, traffic analysis, or regulatory overreach. Additionally, the mere existence of encrypted communication may be sufficient to attract adversarial attention.

A blockchain-based steganographic system offers a paradigm shift in secure government communication. By embedding confidential messages within innocuous blockchain transactions, agencies can transmit secret documents without revealing their existence to external observers.

For instance, police departments could distribute confidential case files or investigative leads by encoding them within blockchain transactions that appear to be routine financial transfers. Military units could coordinate

operations by sharing mission parameters or situational reports using steganographically generated transaction fields. Only parties equipped with the necessary keys and algorithms could reconstruct the messages, while adversaries monitoring the blockchain would see only ordinary transactional activity (Omego and Bosy 4).

The multichannel nature of blockchain networks, combined with hybrid steganographic protocols, further enhances resilience against sophisticated attacks such as replay or man-in-the-middle attacks. By distributing message payloads across multiple transaction fields or even multiple blockchains, the system complicates adversarial efforts to reconstruct complete messages or infer communication patterns (Omego and Bosy 2).

This approach can also facilitate cross-agency collaboration, as the protocol supports secure key exchange and access control, ensuring that only designated recipients can decode specific information.

6. Discussion

Advantages of Blockchain-Based Steganography

The integration of blockchain and steganography offers several compelling benefits:

- **Invisibility of Communication:** By embedding data in transaction fields that are statistically indistinguishable from normal transactions, the existence of covert communication is concealed (Torki et al. 5; Chen et al. 2).
- **Tamper-Resistance and Auditability:** Blockchain's distributed consensus ensures that once a transaction is validated, its contents (including hidden data) cannot be altered or deleted. This is especially valuable for evidentiary chains in law enforcement or the long-term preservation of medical records (Torki et al. 5).
- **Platform Readiness:** Unlike traditional steganography, which often requires the design and deployment of custom platforms for data transmission and storage, blockchain provides a globally accessible, always-on infrastructure (Torki et al. 2).
- **Scalability and Adaptability:** Advanced embedding techniques, including GAN-based field generation and hybrid multichannel protocols, allow the system to scale across varying capacity and concealment requirements (Chen et al. 3; Omego and Bosy 1).
- **Resilience to Steganalysis:** The absence of manual changes and the use of algorithmically generated fields complicate efforts to detect or extract covert messages, even for sophisticated adversaries (Torki et al. 7).

Limitations and Open Challenges

Despite these strengths, several limitations persist:

- **Algorithmic Complexity:** Generating transaction fields that encode specific data bits may require significant computational effort, especially for high-capacity embeddings or large datasets (Torki et al. 5; Chen et al. 3).
- **Detection Risks:** If adversaries discover the specifics of the embedding algorithm or key management practices, they may devise targeted steganalysis techniques to identify or disrupt covert transactions (Torki et al. 7).
- **Trade-offs Between Capacity and Concealment:** Increasing the amount of data embedded per transaction may reduce concealment, as outlier transaction patterns could emerge. Balancing these factors is a continuing area of research (Chen et al. 3).
- **Regulatory and Ethical Considerations:** The use of covert channels for sensitive data may raise legal and ethical questions, particularly in regulated industries such as healthcare or finance.
- **Scalability of Key Management:** Ensuring secure and efficient key distribution and rotation, especially in multi-party settings, remains a practical challenge.

7. Future Directions

Ongoing research is exploring ways to address these limitations. For example, the use of evolving cryptographic functions, adaptive GAN architectures, and decentralized key management protocols may enhance both security and usability (Chen et al. 4; Zhang 3). Additionally, integrating quantum-resistant steganography and leveraging physical phenomena such as DNA-based signatures may offer new frontiers in long-term data authenticity and security (Zhang 3-4).

8. Conclusion

The convergence of blockchain technology and steganography heralds a new era in covert communication and secure data transmission. By embedding hidden messages within the seemingly innocuous fields of blockchain transactions, it is possible to achieve a level of security and privacy unattainable by cryptography alone. The proposed system leverages advanced algorithms to generate transaction fields that encode secret data without manual changes, maintaining the indistinguishability and robustness of the blockchain ledger.

Case studies in medical record management and government document sharing illustrate the practical benefits of this approach, from safeguarding patient privacy to ensuring the confidentiality of national security information. Nevertheless, the field is not without challenges. Balancing capacity, concealment, computational efficiency, and regulatory compliance will require ongoing innovation and interdisciplinary collaboration.

In sum, blockchain-based steganography represents a promising and adaptable framework for secure covert communication in an increasingly interconnected world. As analytical techniques and adversarial capabilities evolve, so too must the algorithms and protocols underpinning this field, ensuring that the hidden channels of tomorrow remain truly invisible.

References

[1] Chen, Zhuo, et al. “Efficient Blockchain-based Steganography via Backcalculating Generative Adversarial Network.” arXiv preprint arXiv:2506.16023v1 (2025). http://arxiv.org/pdf/2506.16023v1

[2] Omego, Obinna, and Michal Bosy. “Multichannel Steganography: A Provably Secure Hybrid Steganographic Model for Secure Communication.” arXiv preprint arXiv:2501.04511v1 (2025). http://arxiv.org/pdf/2501.04511v1

[3] Torki, Omid, Maede Ashouri-Talouki, and Mojtaba Mahdavi. “Blockchain for steganography: advantages, new algorithms and open challenges.” arXiv preprint arXiv:2101.03103v1 (2021). http://arxiv.org/pdf/2101.03103v1

[4] Zhang, Yixin. “Blockchain of Signature Material Combining Cryptographic Hash Function and DNA Steganography.” arXiv preprint arXiv:1909.07914v1 (2019). http://arxiv.org/pdf/1909.07914v1