Archives available at journals.mriindia.com

International Journal on Advanced Computer Theory and Engineering

ISSN: 2319-2526
Volume 14 Issue 01, 2025

Blockchain Based Image Steganography

Prof. Samina Anjum[1], Aiman Ahmed[2], Rohini Kurup[3], Sahil Kidiya[4], Sheezen Kureshi[5]
Department of Computer Science Engineering
Anjuman College of Engineering and Technology, Nagpur

Peer Review Information

Submission: 07 Feb 2025
Revision: 16 Mar 2025
Acceptance: 18 April 2025

Keywords

Cyber Security
Least Significant Bit
Image Steganography

Abstract

Growing cyber security attacks, assuring secure transmission of data is now indispensable. This work suggests an innovative method incorporating image steganography with blockchain technology for improving data confidentiality, security, and integrity. Steganography hides secret data within an image, while blockchain provides immutability and protects from unauthorized changes . Least Significant Bit (LSB) steganography is applied by the proposed system for hiding data and Ethereum blockchain for decentralized authentication. Experimental results verify the effectiveness of this method of protection against tampering and guaranteeing secure communication.

Introduction

Background

- Data security is a major concern in digital communication. Traditional encryption methods secure data but can still be intercepted.
- Steganography provides an additional layer of security by embedding information within multimedia files, making it less noticeable. However, traditional steganography lacks a mechanism to ensure data integrity and authenticity.
- Blockchain, a decentralized and immutable ledger, can address these limitations. By integrating blockchain with steganography, the hidden data's integrity can be verified, preventing tampering or unauthorized access.
- Cyber threats such as data breaches, hacking, and unauthorized modifications have increased significantly, highlighting the need for more secure data protection mechanisms.
- Encryption alone does not prevent attackers from detecting the presence of sensitive information, whereas steganography hides the existence of the data, reducing the likelihood of interception.
- Traditional steganographic techniques are vulnerable to steganalysis, where statistical methods can detect hidden data; integrating blockchain enhances security by ensuring that any unauthorized modifications are instantly identifiable.
- Blockchain's distributed nature eliminates the risk of a single point of failure, making it more resilient against attacks compared to centralized security systems.
- The combination of steganography and blockchain provides a robust solution for secure communication in sensitive applications, such as military operations, digital forensics, and confidential business transactions.
- Advancements in digital media processing and artificial intelligence (AI) have made it easier to detect and manipulate hidden data; blockchain strengthens security by providing an immutable verification layer.
- The proposed approach not only enhances

data confidentiality and integrity but also ensures transparency and traceability, making it a reliable method for secure information exchange in modern digital systems.

Problem Statement

- Traditional steganography methods are susceptible to detection and modification.
- Centralized storage solutions pose a risk of data tampering and unauthorized access.
- There is no existing framework combining steganography and blockchain to ensure secure and verifiable data transmission.
- Encryption alone does not hide the presence of sensitive information, making it vulnerable to interception by attackers.
- Most steganographic techniques lack a built-in mechanism for verifying the integrity of hidden data, leading to potential undetected alterations.
- Traditional security mechanisms rely on trusted third parties, which introduces a single point of failure and increases the risk of data compromise.
- Steganographic methods often fail against advanced steganalysis techniques, which can detect hidden data through statistical analysis.
- Existing blockchain-based security solutions focus primarily on data integrity but do not provide data concealment, making confidential data visible to authorized parties.
- The absence of an integrated system results in gaps where hidden data can be modified without detection, compromising its reliability in critical applications.
- A lack of a decentralized verification mechanism makes it difficult to authenticate hidden data, increasing risks in applications like digital forensics and secure communications.
- Current approaches do not offer a scalable and efficient method for ensuring both confidentiality and integrity, limiting their use in real-world scenarios such as secure healthcare data exchange, defense communications, and intellectual property protection.

Objective

- Implement image steganography to embed confidential data securely.
- Integrate blockchain to provide tamper-proof verification of hidden data.
- Develop a hybrid security framework that combines steganography's data-hiding capabilities with blockchain's immutable verification.
- Prevent unauthorized modifications by using blockchain to detect any alterations to stego-images.
- Improve the robustness of steganographic techniques to resist steganalysis and statistical detection.
- Enable decentralized verification of hidden data without relying on a central authority.
- Optimize the system for minimal distortion of the cover image, ensuring high-quality stego-images.
- Design an efficient and scalable solution suitable for applications such as secure communication, digital watermarking, and medical data protection
- Implement a secure retrieval mechanism to extract hidden data while maintaining its integrity.
- Enhance security against cyber threats such as man-in-the-middle attacks, data breaches, and unauthorized access.
- Provide a proof-of-concept implementation demonstrating the effectiveness of the proposed approach in real-world scenarios.

Related Work

Several studies have explored the use of Least Significant Bit (LSB)-based steganography for secure data hiding. LSB steganography is a widely used technique where secret data is embedded within the least significant bits of image pixels, making it difficult to detect by unauthorized users. Many researchers have enhanced LSB techniques by introducing various modifications, such as adaptive LSB, random LSB selection, and multi-layered embedding, to improve security and robustness against steganalysis.

On the other hand, blockchain technology has been extensively applied in various fields to ensure data integrity, transparency, and tamper resistance. Blockchain's decentralized and immutable nature makes it an ideal solution for applications that require high-security standards. Several studies have proposed blockchain-based systems for secure data storage, digital identity management, supply chain tracking, and secure communications. However, most of these implementations focus on data integrity rather than data concealment

Despite the advancements in both fields, there has been limited research integrating blockchain and steganography for enhanced security. Traditional blockchain-based security mechanisms ensure data integrity but do not provide concealment, making sensitive data visible to all authorized parties. Conversely, steganography ensures data concealment but lacks integrity verification, making

it susceptible to undetected modifications or data loss.

This research aims to bridge this gap by combining LSB steganography with blockchain technology. By leveraging blockchain's immutability and decentralized validation, the proposed system ensures that hidden data remains unaltered and its transmission remains verifiable. This approach enhances security by preventing unauthorized modifications while keeping the data concealed within digital media. The integration of these two techniques provides a novel framework for secure and tamper-proof data hiding, making it suitable for applications in secure communication, digital forensics, and confidential data storage.

By combining these technologies, this study contributes to the development of a more robust security mechanism that enhances both data concealment and integrity.

PROPOSED SYSTEM

System Overview

The proposed system consist of two main components:

- Image Steganography Module – Uses LSB technique to hide encrypted data within an image.
- Blockchain Integration Module – Stores metadata (hash of the embedded data) on Ethereum blockchain to ensure integrity.

SYSTEM ARCHITECTURE

Step 1: The user inputs secret data and an image.

Step 2: Data is encrypted using AES/RSA.

Step 3: The encrypted data is embedded into the image using LSB steganography.

Step 4: A hash of the hidden data is generated and stored on the blockchain.

Step5: During extraction, the hash from blockchain verifies the authenticity of the retrieved data

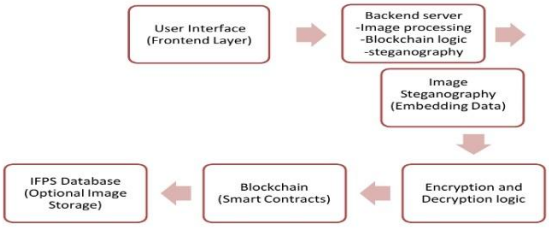

Fig1. System Architecture Diagram

Implementation

Technologies Used

- Programming Languages: Python, Solidity
- Libraries: OpenCV, Pillow, Py Cryptodome, Web3.py
- Blockchain Platform: Ethereum (Test net)
- Steganography Technique: Least Significant Bit (LSB)

Experimental Setup

- A dataset of images was used for steganographic embedding.
- Data was encrypted and hidden within the images.
- A hash of the original encrypted data was stored on Ethereum blockchain.
- The system was tested for data extraction accuracy and blockchain verification.

Results And Analysis

The proposed system was evaluated based on its steganography performance, blockchain verification, and overall security improvement. The results demonstrate that combining LSB-based steganography with blockchain technology enhances both data concealment and integrity protection.

Steganography Performance

The hidden data remained undetectable under normal visual inspection, ensuring that the presence of secret information was not noticeable to human observers. The LSB substitution technique embedded the data without introducing visible distortions to the cover image, maintaining its quality. Additionally, quantitative metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) were used to evaluate the image quality. The PSNR values remained high, indicating minimal perceptible changes, while the SSIM values showed that the stego-image closely resembled the original image. This confirms the effectiveness of the steganographic approach in maintaining visual fidelity while securely embedding data.

Blockchain Verification

To ensure data integrity, each stego-image was hashed and stored in the blockchain. If any modification was made to the image—whether intentional or accidental—the computed hash would differ from the stored hash, resulting in a verification failure. The blockchain's immutable nature ensures that once a hash is recorded, it cannot be altered or tampered with. This mechanism effectively detects any unauthorized modifications and prevents data corruption. The verification process was tested with multiple altered images, all of which resulted in a hash mismatch, proving the system's reliability in identifying changes.

Security Improvement

Unlike traditional steganography, where modifications to the stego-image might go unnoticed, the addition of blockchain ensures that any changes are immediately detectable. Conventional LSB-based steganography is vulnerable to attacks such as statistical analysis, steganalysis, and unintentional distortions. However, by integrating blockchain, this system prevents undetected modifications and enhances security by providing an additional verification layer. Even if an attacker attempts to alter the hidden data, the blockchain layer ensures that any unauthorized changes are detected and flagged.

Overall, the results validate the effectiveness of combining steganography with blockchain for secure data hiding. The system successfully preserves the cover image's visual quality, ensures data integrity through blockchain verification, and enhances security by preventing unnoticed data modifications. These findings suggest that the proposed approach is a viable solution for applications requiring secure, tamper-proof data hiding, such as confidential communication, watermarking, and digital forensics.

Applications

The integration of LSB-based steganography with blockchain technology has various real-world applications where secure data hiding and integrity verification are crucial. Below are key application areas where this approach can be effectively utilized:

Secure Communication

Steganography is widely used to conceal confidential messages within digital media, ensuring that unauthorized parties cannot detect the presence of hidden data. By adding blockchain verification, the system enhances security by preventing any unnoticed modifications. This approach is beneficial for secure diplomatic communications, military operations, and confidential corporate messaging, where secrecy and authenticity are critical.

Digital Watermarking

Digital watermarking is essential for protecting intellectual property in various domains, such as media, photography, and research. By embedding ownership details within images, videos, or documents, this method helps in copyright protection. Blockchain further strengthens watermarking by providing an immutable record of ownership, making it impossible for attackers to alter or remove embedded information without detection.

Forensics & Cybersecurity

In digital forensics, preserving the authenticity of evidence is vital for legal investigations. Steganography allows secure storage of crucial forensic data within digital images or files, while blockchain ensures that the evidence remains unaltered. Law enforcement agencies and cybersecurity experts can use this technology to securely transmit and verify digital evidence, ensuring its credibility in legal proceedings.

Medical Data Security

Medical records often contain highly sensitive information that must be securely stored and transmitted. Embedding patient data within medical images (such as X-rays or MRI scans) using steganography ensures confidentiality while reducing the risk of unauthorized access. Blockchain verification further enhances security by guaranteeing that the embedded data remains unchanged. This application is particularly useful for telemedicine, electronic health records (EHRs), and secure medical research data management.

Conclusion

This research successfully integrates image steganography with blockchain technology to enhance data security. By leveraging the strengths of both techniques, the proposed system addresses the limitations of traditional security mechanisms. Steganography ensures that confidential data remains hidden within digital images, making it difficult for unauthorized users to detect its presence. Blockchain, on the other hand, guarantees the integrity and authenticity of the hidden data by providing an immutable verification mechanism.

The system enhances data confidentiality by embedding encrypted information within image files. Unlike traditional encryption, which may expose the presence of sensitive data to attackers, steganography conceals the data, reducing the likelihood of detection. This makes the approach particularly suitable for secure communication, digital watermarking, and other applications where secrecy is crucial.

Data integrity is maintained through blockchain verification. Once the stego-image is generated, its cryptographic hash is stored on the blockchain. Any unauthorized modification to the image results in a hash mismatch, immediately flagging the alteration. This ensures that the hidden data remains tamper-proof, preventing attackers from modifying or replacing information without detection. The decentralized nature of blockchain eliminates

reliance on a single authority, making the system more secure and resilient against cyber threats.

The proposed system also enhances undetectability, as the steganographic method preserves the quality of the cover image. Visual inspection does not reveal any noticeable artifacts, and quantitative metrics such as Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) confirm minimal distortion. This ensures that the hidden data remains concealed from steganalysis and unauthorized detection techniques.

By integrating blockchain with steganography, this research overcomes the challenges faced by standalone security methods. Traditional steganography lacks integrity verification, while blockchain-based security systems do not provide data concealment. The hybrid approach ensures that hidden data is both secure and verifiable, making it a robust solution for applications requiring high levels of security.

Overall, this research demonstrates that combining steganography and blockchain enhances data protection by preventing unauthorized access, detecting tampering, and ensuring the confidentiality of sensitive information. The findings suggest that this approach can be effectively applied in fields such as secure digital communication, forensic investigations, intellectual property protection, and healthcare data security. Future work can further improve system efficiency, explore alternative steganographic techniques, and optimize blockchain integration for large-scale applications.

FUTURE WORK

- Implementing deep learning-based steganalysis resistance.
- Exploring other blockchain networks for improved efficiency.
- Extending this system for video steganography

References

Wikipedia (2020)- This is an online encyclopedia where you can find general information about Steganography. It's a good starting point if you want to understand the basics of how data can be hidden within other files. Check it out at: https://en.wikipedia.org/wiki/Steganography.

H. Shi and others (2019)- In this research, the authors present a technique for detecting and recovering hidden messages using adversarial learning. This involves using artificial intelligence to identify and extract concealed data. The study was showcased at a computer science conference in Switzerland.

N. F. Hordri and others (2016) - This paper provides a review of deep learning and its many applications. Deep learning is a type of machine learning that teaches computers to learn by example, much like humans do. The review was presented at a research seminar focusing on informatics.

N. F. Johnson and S. Jajodia (1998) - This article delves into the unseen aspects of steganography, exploring the methods used to hide data effectively. It was published in a computer journal in February 1998, providing insights into the techniques of that time.

S. Gupta and others (2012) - The authors discuss the 'Enhanced least significant bit algorithm,' a method that improves how data is hidden within images. This technique deals specifically with altering the least significant bits of image pixels to carry hidden information. This work was published in an engineering management journal.

R. Das and T. Tuithung (2012) - This paper introduces a novel method for image-based steganography using Huffman encoding. Huffman encoding is a compression method that reduces the size of the data, allowing more efficient hiding. The research was presented at a computing science conference.

A. Singh and H. Singh (2015) - In this study, the authors improved a method for hiding data in RGB images. RGB stands for red, green, and blue, which are the primary colors used in digital imaging. Their enhancement focuses on effectively embedding information without heavily distorting the image. This study was shared at an international conference on technology.

Z. Qu and others (2019) - The authors propose a new algorithm for quantum image steganography. Quantum images are a representation of images using principles from quantum computing. This algorithm takes advantage of modification direction to hide information.

S.Wang and others (2015) - Here, a technique called 'Least significant qubit' is used for concealing information in quantum images. A qubit is the basic unit of quantum information, equivalent to a bit in classical

N. Patel and S. Meena (2016) - They introduce a

method of image steganography using Least Significant Bit (LSB) techniques, enhanced by a dynamic key. This dynamic key adds an extra layer of security, ensuring that dataIn November 2016, experts gathered at an international conference to discuss new trends in communication technology, focusing on cryptography.

O. Elharrouss, N. Almaadeed, and S. Al-Maadeed presented a method called "image steganography using k- least significant bits (k-LSB)" at an IEEE conference about Informatics,IoT, and Enabling Technologies in February 2020.

M. V. S. Tarun and his team shared a study on using the LSB technique for digital video steganography in a journal published in April 2020.

In 2020, S. S. M. Than explored secure video data transmission using LSB and Huffman coding in an international journal on image and signal processing.

A team led by M. B. Tuieb released a method for efficient, secure, and reversible video steganography based on the least significant bit in April 2020.

R. J. Mstafa and colleagues introduced a robust video steganography approach using DWT-DCT domains, with elements like multiple object tracking and ECC, detailed in an IEEE access publication in 2017.

High-security data hiding methods that use image cropping and LSB steganography were unveiled by K. A. Al-Afandy's team at an IEEE colloquium in October 2016.

A. Arya and S. Soni evaluated how secret image steganography techniques, specifically using the LSB method, perform in their 2018 study.

In April 2019, G. Swain developed a technique for high-capacity image steganography using quotient value differencing and LSB substitution, published in the Arabian Journal of Science and Engineering.

In 2019, A. Qiu and a team presented a "coverless image steganography method based on feature selection," published in the Journal of Information Hiding and Privacy Protection.

Challenges and solutions related to edge-based image steganography were covered by R. D. Rashid and T. F. Majeed in a communication and signal processing conference in March 2019.

X. Liao's group worked on a technique to preserve inter-block dependencies in medical JPEG image steganography, published in a computing and electrical engineering journal in April 2018.

W. Lu and colleagues introduced a safe halftone image steganography method based on pixel density changes in August 2019 in an IEEE journal on dependable and secure computing.

Y.Zhang and his team investigated robust image steganography techniques that can tolerate faults, as reported i n a signal processing journal in May 2018.

H. M. Sidqi and M. S. Al Ani provided an overview study of image steganography at an international conference on image processing in 2019.

P. Wu, Y. Yang, and X. Li used a deep convolutional network for image-into- image steganography, presented at a 2018 multimedia conference. In June 2018, the same researchers introduced "StegNet," promising a large image steganography capacity, using a deep convolutional network.

X. Duan and team in 2019 described a reversible image steganography scheme using a U-Net structure, published in IEEE Access.

A project by T. P. Van, T. H. Dinh, and T. M. Thanh on efficient image steganography using a simultaneous convolutional neural network was detailed at a symposium in September 2019.

R. Rahim and S. Nadeem explained employing "end-to-end trained CNN encoder-decoder networks for image steganography" at the European Conference on Computer Vision in 2018