Received: 2025-08-04
Accepted: 2025-09-03
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

A Hybrid Approach to Data Security Using Steganography and Blockchain for Tamper-Proof Communication

Prashant*[1], [2]Shashank Jha[2], Beer Singh[3], Gesu thakur[4]

[1,2]Assistant Professor, Department of Computer Science and Application,
COER University, Roorkee, India.
[3]Assistant Professor Department of Computer Application, SRMCEM College
Lucknow, India
[4]Professor & Head, Department of Computer Science and Application,
COER University, Roorkee, India
***Corresponding Author:** prashantshrivastav644@gmail.com

Abstract

In the data security the cryptography and steganography could be usefull for data security individually. But individual these security techniques are not enough to provide sufficient data security. In this paper we have shows that steganography and blockchain are used together to hide encrypted data inside image. The proposed method will solve two major drawbacks of the current existing security techniques, the large size of ciphertext imbedded into an image and other is to provide integrity and authenticity are guaranteed by blockchain, because it provide unalterable ledger and cryptographic hashes. Tamper detection will guaranteed through verification of the extract messages's hash against blockchain data.

Keywords: steganography, cryptographic, blockchain, Hybrid Approach, Tamper-Proof Communication.

Introduction

The revolution in the digital age has brought about an exponential growth in data generation, transmission and storage. Along with this boom, the risk of data breaches, unauthorized tampering and cyber-attacks has also grown manifold. Conventional security measures including encryption and password-based authentication provide protection but are frequently vulnerable to attacks and exposing sensitive information to threats. The requirement for a more sophisticated and multi-layered security infrastructure has never been more imperative. This paper discusses a new method that combines blockchain technology and steganography to ensure greater data security, ensuring both confidentiality and integrity [1].

Blockchain, an immutable and decentralized ledger, has emerged as a game-changing technology for securing digital transactions. Blockchain stores data in a way that makes it impossible to alter without being detected, thus offering a robust mechanism for verification[2]. Every transaction or data entry is encoded in a block and cryptographically linked to the previous one, providing a secure and open record of information. Blockchain was first created to handle financial transactions but has been used across other areas, including healthcare, supply chain managementand secure communication[3].

Steganography is a well-established technique for hiding information in digital media, such as images, audio, and video. Unlike encryption, which transforms data into unreadable format to prevent unauthorized access, steganography conceals information in an invisible manner for the human eye[4]. This undetectable property renders it an extremely useful secure communication and protection method for sensitive data. While traditional steganography techniques rarely include an efficient method of verification, this drawback curtails its suitability for applications with security demands[5][32].

The combination of blockchain and steganography overcomes the weaknesses of both systems by synergizing their strengths. In the system under consideration, sensitive information is hidden in images through steganography and a linked cryptographic hash is stored in the blockchain. This protects against any unauthorized changes in the image to be detected by checking the stored hash. When an image is tampered with, its derived data will no longer be equal to the original hash indicating possible tampering [6].

A. Importance of Data Security Using Blockchain and Steganography

First, it offers another layer of protection, making unauthorized access and tampering much harder.

Second, the blockchain ledger promotes transparency and accountability since all changes are logged and can be traced. Finally, blockchain's decentralized nature prevents the risks of centralized storage, reducing the probability of single-point failures [7].

The present work intends to give a holistic description of the intended system, covering its execution, performance, and applications. With the help of blockchain to authenticate integrity and steganography for hiding data, this study enhances the methodology of secure storage and transmission methods for data [8]. The subsequent parts of this article will discuss methodology, system architecture, experimental findings, and implications on a large scale of the new security system [9][33].

B. **Problem Definition:** In the current digital environment, protecting sensitive data is still a major challenge. Conventional data protection methods, like encryption and password authentication, are effective but vulnerable to security attacks, such as hacking, data tampering, and unauthorized access. Centralized data storage systems also present a major threat, as a single point of failure can result in massive data loss or exposure [10].

The issue comes in because a safe, verifiable, and decentralized way of holding and carrying out confidential data has to be ensured. Present cryptography methods guard information by rendering it inaccessible to non-authorized personnel, but intercepted, the mere existence of encrypted data may be an indication of sensitive information. Steganography tries to meet this demand by hiding information inside digital media such that it will be hidden from possible intruders. Nevertheless, conventional steganographic techniques have weak verification mechanisms, exposing hidden information to tampering without evidence [11].

C. **Key components of the problem definition include:**

- **Confidentiality:** Protect sensitive information from disclosure to unauthorized parties via steganographic embedding.
- **Integrity:** Guard against illicit tampering by storing cryptographic hashes on a blockchain.
- **Decentralization:** Disallow single points of failure through the distributed nature of blockchain.
- **Tamper Detection:** Support effective verification of data integrity to identify any illegal alterations.

By solving these problems, the designed system can improve data security in some applications, like secure documentstorage, confidential communication, and digital watermarking. The following sections will present more details about the methodology, implementation, and experimental validation of this security scheme.

RELATED WORK

Blockchain and steganography integration has been investigated through many studies that all pointed to the advantages and limitations of using these technologies for the protection of digital data. The following overview offers a look into some notable research contributions concerning blockchain-based security, steganography methods, and their implementation in combination [12][30].

The technology of blockchain has become so well known today because it's decentralized and non-alterable. It makes sure that as soon as data is written, it cannot be changed without agreement, which renders it extremely resistant to tampering. Different research has proven the efficiency of blockchain in protecting sensitive information in a variety of areas. For example, Chowdary[4] presented blockchain in the context of Bitcoin, proving its ability as a safe and open ledger system. Follow-up studies have investigated blockchain uses in healthcare, financial transactions, supply chain management, and identity verification.

Sharma et al. [6] has explained how blockchain's decentralized structure eliminates the necessity of a central authority, thus minimizing risks of centralized storage systems. Recent developments have also suggested hybrid blockchain architectures that improve security while maximizing transaction speeds, which are appropriate for real-time applications. Nevertheless, blockchain itself is not a promise of confidentiality, as every transaction entered on an open ledger can be seen by members of the network. This restriction calls for the combination of supporting security methods like steganography.

Steganography has been extensively studied as a technique for hiding secret information in digital media, so that data is not accessible to unauthorized users. Steganography does not make data inaccessible to unauthorized users, as encryption does, but hides the fact that data is present. Several steganographic techniques have been proposed, such as spatial domain techniques such as Least Significant Bit (LSB) manipulation and frequency domain techniques such as Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

Adee and Mouratidis [8] offered a pioneering investigation into digital steganography, presenting its capability in secret communication. Subsequent investigations presented better algorithms to enhance capacity for payload along with image integrity. For instance, Abbas et al. [9] presented a steganographic process that further advance security through incorporation of cryptographic encryption prior to inserting data. However, a basic problem of many steganographic systems is insufficient verification mechanism that leaves them at risk of detection-free alterations [24].A smart grid relies on advanced metering infrastructure techniqus, which improves intrusions, a novel fog-edge-enabled federated SVM-based enhanced intrusion detection system has been proposed. It improves accuracy and efficiency and protecting user data using outperforming traditional methods on NSL-KDD and CICIDS2017 datasets [25]. The evolution of IoT and 5G sets the backbone for 6G technology for ultra-fast data, low latency and edge intelligence technology. The digital technology cover the gap between real time monitoring and data communication, a enhanced federated learning DT technology has been introduced for securing 6G operations in smart cities[26]. The lack of digital security in automated housing societies, author proposes to keep secure automated housing society using IoT and networking simulated via Cisco Packet Tracer and connected homes, power stations and banks with IoT devices using routers, switches, VLSM-based IP addressing [27].

S.No	Authors (Year)	Title/Focus	Key Contribution	Source
1	Rajguru et al. [1]	Steganographic approaches for cloud security	Proposed multiple steganographic methods to improve cloud data confidentiality	E3S Web of Conferences
2	Arunachalam et al. [2]	Cybersecurity framework for time dissemination	Developed a national cyber framework for secure time sync	SN Computer Science
3	Wang et al. [3]	Deep learning for steganography	Survey of deep learning-based data hiding unifying steganography and watermarking	arXiv
4	Chowdary et al. [4]	Steganography in speech signals	Audio steganography integrated with encryption for secure communication	arXiv
5	Prashar et al. [5]	Review on data security challenges	Survey of current cybersecurity challenges, including steganography	Springer
6	Sharma et al. [6]	Healthcare cybersecurity	Discussed steganography in context of healthcare information security	Springer
7	Jajodia et al. [7]	Encyclopedia entry	Comprehensive coverage on cryptography, steganography and security techniques	Springer

8	Adee&Mouratidis [8]	Cloud data protection	Proposed 4-step model using steganography and cryptography	Sensors
9	Abbas et al. [9]	Hybrid crypto-stegano for cloud	Presented a hybrid security system combining steganography and cryptography	IEEE
10	Madavi&Karthick [10]	Enhanced cloud security	Combined encryption and steganographic methods for data protection	IEEE
11	Pant et al. [11]	Three-step model	An early hybrid model integrating RSA and steganography for cloud	IEEE
12	Chatterjee et al. [12]	Secure LMS	Cloud LMS security enhanced with encryption and steganography	Wireless Personal Communications
13	Dudiki et al. [13]	Hybrid cryptography	Introduced cryptographic algorithm with potential for steganographic integration	IEEE
14	Abel et al. [14]	Crypto-stegano in cloud	Secure data embedding method for cloud using both techniques	Springer
15	Pandey et al. [15]	ML for cloud security	Studied machine learning roles in cloud security, touching steganography use	IEEE

A. Blockchain and Steganography Integration

The integration of blockchain and steganography has been suggested as a new method of overcoming their respective limitations. A number of studies have identified how blockchain can be used as an immutable verification layer for steganographically hidden data, such that any unauthorized changes are identifiable.Pant et al. [11] proposed a blockchain-based steganography authentication system, where cryptographic hashes of secret messages were stored on the blockchain. The method allowed users to recover and authenticate hiddendata without revealing it to third parties. Chatterjeeet al.[12] also conducted a study on an optimized blockchain-steganography framework for secure document storage, proving enhanced security and efficiency over conventional encryption-based schemes.

Despite these advancements, challenges remain in optimizing blockchain performance, reducing computational overhead, and improving steganographic robustness against attacks. Future research aims to address these issues by incorporating artificial intelligence for adaptive security measures anddeveloping lightweight blockchain protocols for faster transaction validation.

BACKGROUND WORK

A. Block Chain

Blockchain is a ground – breaking technology that facilitates the creation of distributed and decentralized databases, where information is stored as an ever-expanding chain of records called blocks. Each block contains a cryptographic hash of the previous block, a timestamp, and the actual data, forming an immutable and tamper-resistant ledger. This cryptographic linkage ensures data consistency and prevents unauthorized manipulation-altering even a single bit would require recalculating the hashes of all subsequent blocks, which is computationally infeasible[13][28].

Originally developed to support financial transaction, blockchain technology has since evolved to support a wide range of applications, including supply chain tracking, secure data logging, healthcare, and digital identity management. Its strength lies in tis ability to provide verifiable, auditable, and transparent records without relying on a central authority, making it highly suitable for systems that demand trust, integrity, and resilience against tampering [14].

the uses of blockchain technology are growing exponentially in the field of cybersecurity. Many researchers have worked with blockchain technology to reduce cyber security in the field of finance, audit reliability, regularity and education. In the year of 2008, NakaMoto has introduced a concept of blockchain which works on decentralized ledger technology and support peer-to-peer transactions without intermediate alteration [15].

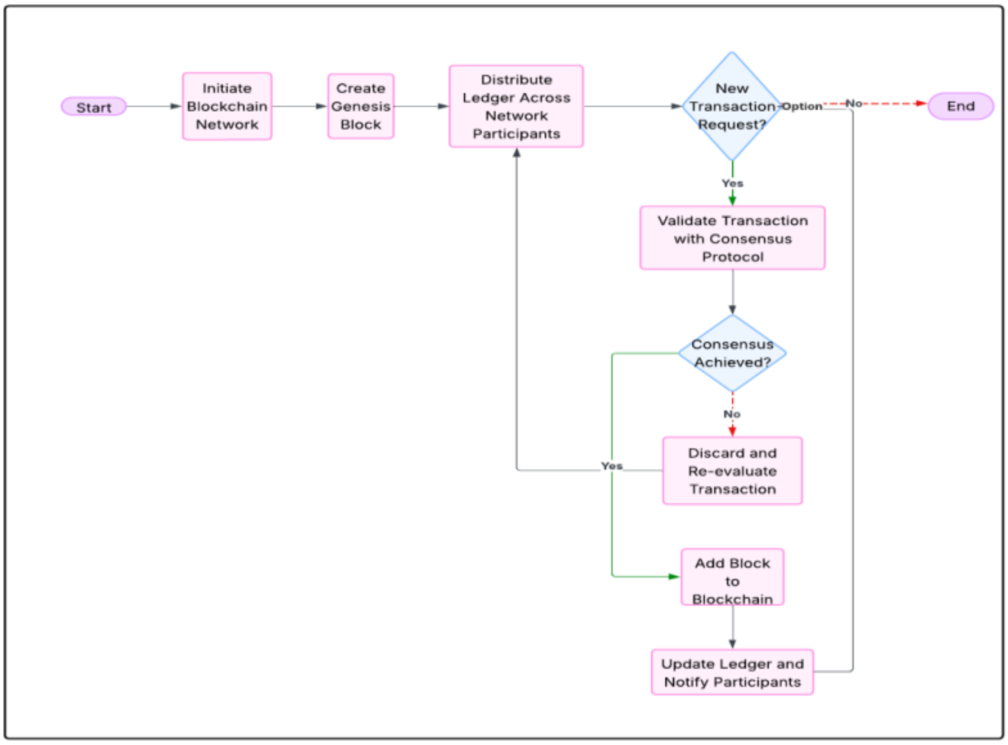

Start
Initiate Blockchain Network
Create Genesis Block
Distribute Ledger Across Network Participants
New Transaction Request?
Option
No
End
Yes
Validate Transaction with Consensus Protocol
Consensus Achieved?
No
Discard and Re-evaluate Transaction
Yes
Add Block to Blockchain
Update Ledger and Notify Participants

Fig 1. Working diagram of Blockchain

Received: 2025-08-04
Accepted: 2025-09-03
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

The fig 1 lustrated the working of blockchain technology. In the first step, the process is started and initiated the blockchain network for setting the foundation for transaction. In the next step, create the first block (also known as Genesis block), which has no previous block address[16]. Now current state of blockchain ledger is shared with all networks. In the next step, a decision is made and check is there a new transaction request arises, if yes then proceed to validate the transaction otherwise end the process. The new transaction is verified using a consensus algorithm, this validate that all the participants agreed with the transaction and check the transaction is valid or not. The next decision point checks the transaction is approved or not if the transaction is discarded, it will be re-evaluated till approved [17]. The invalid or unapproved transaction will re-examine or discarded and if transaction is approved, the transaction is added as a new block of blockchain. All nodes are updated with the new blockchain states. Now updated block is distributed again and ready for the next transaction [18][29].

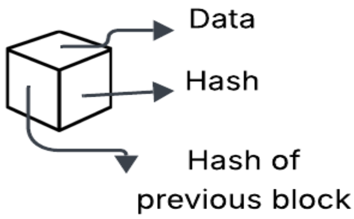


Fig 2. Architecture of Block in Blockchain

The fig 2 illustrated that the block of block chain which contains three types of storage section, in first section contains data and the second section contains the hash value of that data and the last section contains the hash of previous data.

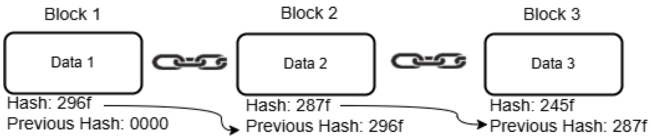


Fig 3. Architecture of Chain in Blockchain

The fig 3 depicted that the chain in blockchain, in which block 1 contains the hash value of previous block, in this case block 1 is a starting block has not previous block so it contains 0000, and the block 1 has its own hash 296f of data 1, the block 2 contains data 2 and also contains the hash value of data 2 that is 287f and previous block's hash value that was 296f. This process creates a chain of hash values.

A. Steganography Technology

Steganography is the art of concealing information within digital media such as images, audio, or video, offering confidentiality by hiding the very existence of data. Unlike encryption, which scrambles data, Steganography embeds it imperceptibly- commonly using Least Significant Bit (LSB) techniques [19]. While effective in hiding information,traditional methods lack verification mechanisms, making them vulnerable to tampering.

Recent Research explores integrating blockchain with steganography to enhance data integrity, leveraging blockchain's decentralized and tamper-proof nature. Successful steganographic systems must ensure imperceptibility, security, capacity, and robustness, with digital images being the preferred medium for embedding secret data without compromising quality[20].Face recognition technologies based on image data have also adopted similar media embedding strategies for maintaining security and image fidelity [35].

Steganography is classified into two categories, first is pure steganography and the second is symmetric and asymmetric steganography. In pure steganography, it does not work on exchange of information while symmetric or asymmetric steganography works on exchange of information and need the security key before sending a message[21]. The steganograpy is totally depends on type of medium being used including text, images, audio-files and network protocols used in network communication [22].

Image steganography is categorized according to working area like spatial domain and frequency domain, in spatial domain steganography works directly on image pixel value and able to change the pixel gray-value and in frequency domain, the image will first convert into frequency domain and then message arecombined in the coefficients [23].

PORPOSED MODELLING

The proposed system has tested the combination of blockchain and steganogrpahy as a solution for each method's have been proposed previsouly. Steganography hides information with confidentiality, where asblockchain verifies the integrity and authenticity with cryptographic hashing functions. This proposed system provides two-tiered security mechanism and proved authenticity and confidentiality of data. The older system was not able to provide convenient integration or speedy verification processes in many cases.

The suggested system enhances current ideas by strongly coupling blockchain and LSB-based steganography. The Secure Data System initially hides secret messages in images through steganographic encoding. It next stores the metadata and a SHA-256 hash of the concealed content in a blockchain ledger. At verification time, the system retrieves the data from the encoded image and verifies it against blockchain records to establish authenticity. This dual method guarantees confidentiality (through steganography) and integrity (through blockchain), ensuring strong protection against tampering and unauthorized access.Earlier video-based security models explored classification through embedded frames, a foundational approach to the current hybrid method [36].

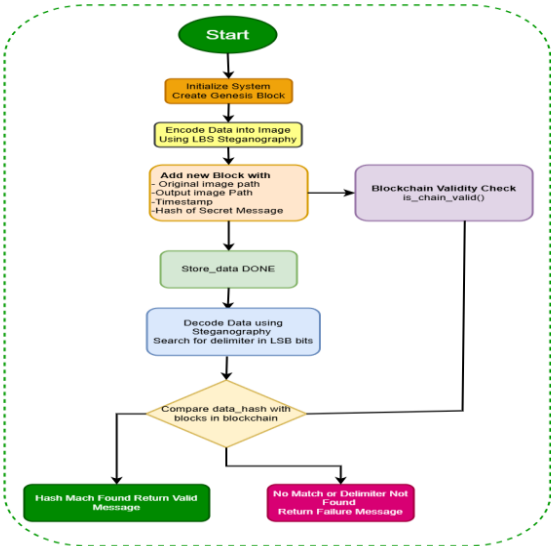


Fig. 4 Flow Diagram of Proposed Algorithm

A. **Pseudocode of proposed model**

1. Initialization (Secure Data System**)**

- Creates a new Blockchain instance.
- Generates the **genesis block** (Block 0).

2. Store Data (store data**)**

1. **Steganography Encoding**:
    - Input: image_path, secret_data, output_path
    - Converts secret_data → **binary** (text_to_binary).
    - Embeds binary data into the image using **LSB steganography**:
    - Modifies the **least significant bit (LSB)** of each pixel's RGB values.
    - Adds a **16-bit delimiter** (1111111111111110) to mark the end.
    - Saves the modified image as output_path.
2. **Blockchain Recording**:
    - Creates a **block** with:
        - image_path (original image).
        - output_path (encoded image).
        - timestamp (current time).
        - data_hash (SHA-256 hash of secret_data).
    - Adds the block to the blockchain.

3. Verify Data (verify_data)

1. **Steganography Decoding**:
    - Extracts **LSBs** from the encoded image.

Received: 2025-08-04
Accepted: 2025-09-03
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

- Converts binary → text (binary_to_text).
- Uses the **delimiter** to identify the end of the hidden message.

2. **Blockchain Verification**:
    - Computes the **SHA-256 hash** of the decoded data.
    - Searches the blockchain for a block with a matching data_hash.
    - If found → **valid** (returns decoded data + blockchain proof).
    - If not found → **invalid** (data tampered or not recorded).

4. Blockchain Integrity Check (is_chain_valid)

- Validates the entire blockchain by:
    - Checking **hash consistency** (recomputing hashes).

Ensuring **previous_hash links** are unbroken.

B. Mathematical Formulation

1. **Message Encoding:**The encoding of the message is the process of hiding secret text data inside an image file using steganography. Unlike traditional encryption process which transform secret message into ciphertext but these approaches are not able to provide sufficient security but due to steganography the secret message conseals within an image's pixels and if anyone look at these image through naked eyes, it looks like unchanged images. But before hiding the secrete message in image, it must be convert into a format that can be embedded within an image pixels.

Binary Conversion

$$B = bin(M) = \bigcup_{i=1}^{|M|} bin(M_i)(1)$$

Add Delimiter

$$B' = B||D \qquad (2)$$

Pixel-level LBS Embedding,
Let $P_{i,j,k} \in I$ be the pixel at position (i,j) and color channel $K \in \{R, G, B\}$. Then

$$P'_{i,j,k} = P_{i,j,k} \land 254 \lor b\text{where}b \in B'(3)$$

Repeat for all bits $b \in B'$ to get:

$$I' = LSB\_Encode(I, B') \qquad (4)$$

2. **Blockchain Hashing & Block Creation**
Each block B_i is a 5-tuple:

$$B_i = (i, h_{i-1}, T_i, D_i, h_i)(5)$$

Where

- i= block index
- h_{i-1}= previous block's hash
- T_i= timestamp

Received: 2025-08-04
Accepted: 2025-09-03
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10103

- D_i=data (includes image path and H(M))
- h_i =$H(i||h_{i-1}||T_i||D_i)$

the genesis block B_0 is:

$$B_0 = (0,"0",To,"GenesisBlock",H(0||"0"||To||"GenesisBlock")) \quad (6)$$

3. **Verification Function**

Image Decoding

$$Bd = Extract\_LSB(I')(7)$$
$$M' = bin^{-1}(Bd[:index(0)])(8)$$

Hash comparison

$$H(M') \overset{?}{\Rightarrow} H(M) \in \{B_i.D_i[\text{data\_hash}]\} \quad (9)$$

If match is found, return “Valid” else “Invalid”,

4. **Final System composition**

The system S can be expressed as a composition:

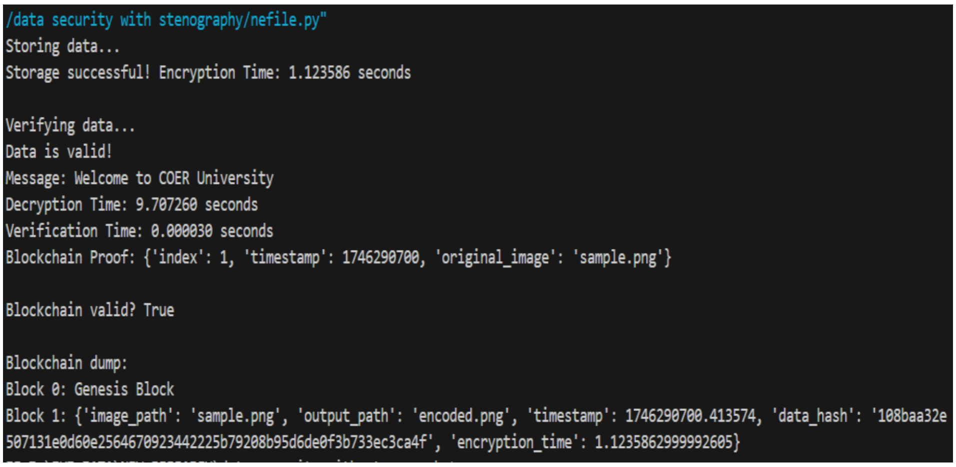
$$S(M,I) = \{^{True,Validated,if\,\exists B_i \in C:H(M')=B_i.D_i[\text{data\_hash}]}_{False,NotFound,Otherwise}(10)$$

RESULTS AND DISCUSSIONS

The proposed systemcombines steganography with blockchain technology to provide data confidentiality and integrity in secure communication. The combination creates a two-tiered security mechanism—hiding sensitive information in digital media (with LSB steganography) and ensuring authenticity and unalterability of that information through a decentralized blockchain ledger. The fig 4 shows that the output of the proposed mode, in which “**Welcome to COER University**” is a messege. We have encrypted the message and embed the ciphertext inside an image “**sample.png**”. The encryption of message and combination in image takes 1.123586 seconds.

Received: 2025-08-04
Accepted: 2025-09-03
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

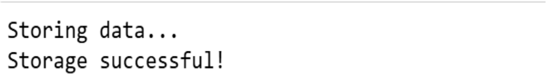


```
/data security with stenography/nefile.py"
Storing data...
Storage successful! Encryption Time: 1.123586 seconds

Verifying data...
Data is valid!
Message: Welcome to COER University
Decryption Time: 9.707260 seconds
Verification Time: 0.000030 seconds
Blockchain Proof: {'index': 1, 'timestamp': 1746290700, 'original_image': 'sample.png'}

Blockchain valid? True

Blockchain dump:
Block 0: Genesis Block
Block 1: {'image_path': 'sample.png', 'output_path': 'encoded.png', 'timestamp': 1746290700.413574, 'data_hash': '108baa32e
507131e0d60e2564670923442225b79208b95d6de0f3b733ec3ca4f', 'encryption_time': 1.1235862999992605}
```

Fig 4. Output of the Proposed Model

A. Data Storage process: When the system runs, it starts by inserting a secret message (e.g., "Welcome to COER University") into a digital image (sample.png) by applying the Least Significant Bit (LSB) steganography technique. The technique is subtle in that it alters the pixel values of the image without significantly impacting its visual look. The output is an encoded image (encoded.png) whose visual appearance is no different from the original image but has the embedded message.

The process output**:**



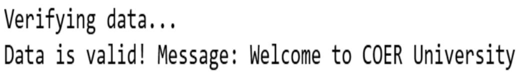
```
Storing data...
Storage successful!
```

Fig. 5: Output of Data Storage

B. Data Verification and integrity checking

After hiding the data, the system goes on to recover and authenticate the message through a hash-based integrity verification. The cryptographic hash (SHA-256) of the concealed message is computed and compared to the stored hash in the blockchain.

The output proves that the message was retrieved successfully and its hash agreed with the stored value in the blockchain. This guarantees that the data has not been altered while being transmitted or stored.



```
Verifying data...
Data is valid! Message: Welcome to COER University
```

Fig. 6 BlockchainVerification

C. Blockchain Record structure

The blockchain is a tamper-resistant record that holds metadata regarding the steganographic process. It starts with a Genesis Block (block 0), i.e., the parent of the chain, and then block 1 containing the information of the transaction

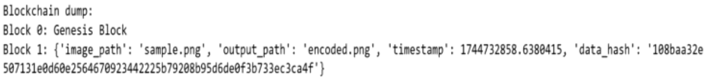
Received: 2025-08-04
Accepted: 2025-09-03
Published Online: 2025-09-20
DOI: 10.70454/JRIST.2025.10103

Journal of Recent Innovation in Science and Technology
E-ISSN: 3117-3926

This document consists of:

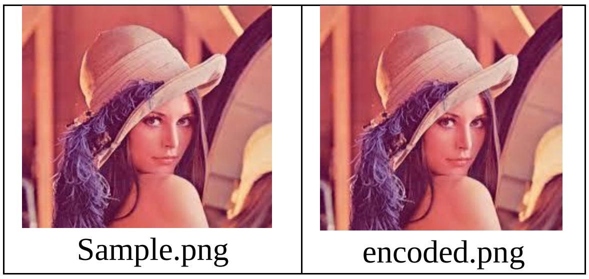
- Paths to original and output images for reference,
- Timestamp of the action,
- A SHA-256 hash of the secret data to confirm integrity.

It would be impossible to change the image or message without causing a discrepancy in the hash, and the system would mark the data as invalid.



```
Blockchain dump:
Block 0: Genesis Block
Block 1: {'image_path': 'sample.png', 'output_path': 'encoded.png', 'timestamp': 1744732858.6380415, 'data_hash': '108baa32e
507131e0d60e2564670923442225b79208b95d6de0f3b733ec3ca4f'}
```

Fig7. Output of the Genesis Block



Sample.png

encoded.png

Fig 8. Image Difference between Before and After Message Encoded

The fig 8 shows that the encrypted message has been combined with imgeLSB, which is pixel level combination. The above images have no difference at visual, but the pixels of both images have been changed.

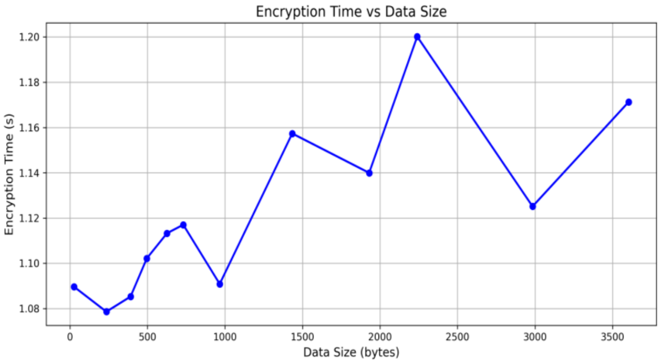


Fig 9. Encryption Time Computation

The fig 9 shows that the encryption computation time of the proposed algorithm. The 26 bytes size of data takes 1.089 seconds encryption time. The encrypted data embed with image LSB and create an new image that looks like same as previous. The fig 10 shows the decryption time of proposed algorithm. The same size of data embeds with image takes 9.160 seconds. The taken time combine with verification as well as decryption time.

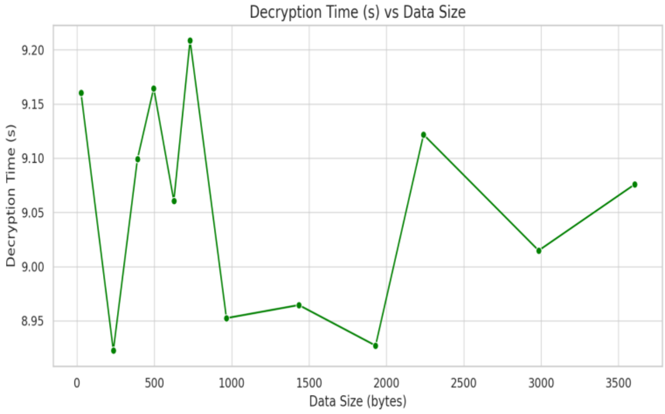


Fig 10. Decryption Time Computation

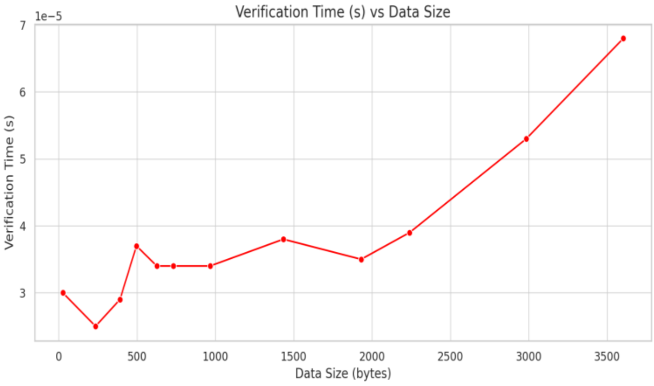


Fig 11. Verification Time Computation

The fig 11 shows the varification computation time taken by the proposed algorithm.The varification process combine with two steps first is decoding and other is varification. During the decoding, extract the LSBs from the encoded image and convert the binary to text. Use the delimiter to identify the endof the hidden message. The vairfication section compute the SHA-256 hash value of decoded message and search blockchain for a block with a matching hash value. If the hash value get matched, it return the decoded data with blockchain proof, Otherwise data got tampered no record found.

The fig 12 shows the time comparison between encryption, decryption and verification. The verification takes less time as compared to encryption and decryption.

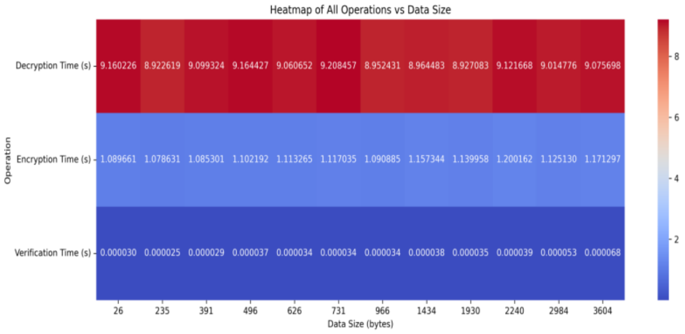


Fig 12. Time Computation graph of encryption, decryption and verification

CONCLUSION

The proposed model authenticate the combining of steganography with blockchain technology can significantly improve the data communication between two parties. The method effectively solves two major problems with traditional methods: the size limits of embedded ciphertext and the lack of data integrity and authenticity. It does this by embedding encrypted data in images and using blockchain's unchangeable record and cryptographic hashes. GAN-based approaches for synthetic secure datasets in mobile health have also shown promise in testing tamper-proof validation layers [34].This integration guarantees safe data transfer with dependable tamper detection, making it a hopeful answer for modern secure communication systems.

References

[1] Rajguru, S. S., Singh, G., Malhi, S. S., &Kaur, G. (2024). Stenographic Approaches for Enhancing Data Security in Cloud Computing. *In E3S Web of Conferences* (Vol. 556, p. 01012). EDP Sciences.https://doi.org/10.1051/e3sconf/202455601012

[2] Arunachalam, A., Seetharaman, K., &Agarwal, A. (2021). Design and Development of a Cyber Security Framework for National Time Dissemination. *SN Computer Science*, 2, 1-12.https://doi.org/10.1007/s42979-021-00471-5

[3] Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., ...&Xue, M. (2023). Data hiding with deep learning: A survey unifying digital watermarking and steganography. *IEEE Transactions on Computational Social Systems*, 10(6), 2985-2999.https://doi.org/10.1109/TCSS.2023.3268950

[4] Chowdary, H., Karan, K., Bharath, K. P., & Kumar, R. (2018, May). Data hiding in speech signal using steganography and encryption. *In 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 1219-1223). IEEE.https://doi.org/10.1109/RTEICT42901.2018.9012508

[5] Prashar, N., Hooda, S., & Kumar, R. (2022, December). Current status of challenges in data security: A review. In International conference on cybersecurity in emerging digital era (pp. 3-13). *Singapore: Springer Nature Singapore*.https://doi.org/10.1007/978-981-99-5080-5_1

[6] Sharma, D. P., HabibiLashkari, A., &Parizadeh, M. (2024). Data and Information Security. In Understanding Cybersecurity Management in Healthcare: Challenges, Strategies and Trends (pp. 55-83). *Cham: Springer Nature Switzerland*.https://doi.org/10.1007/978-3-031-68034-2_4

[7] Jajodia, S., Samarati, P., & Yung, M. (Eds.). (2019). Encyclopedia of Cryptography, Security and Privacy.https://doi.org/10.1007/978-3-030-71522-9_300005

[8] Adee, R., &Mouratidis, H. (2022). A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. *Sensors*, 22(3), 1109.https://doi.org/10.3390/s22031109

[9] Abbas, M. S., Mahdi, S. S., &Hussien, S. A. (2020, April). Security improvement of cloud data using hybrid cryptography and steganography. *In 2020 international conference on computer science and software engineering (CSASE)* (pp. 123-127). IEEE.https://doi.org/10.1109/CSASE48920.2020.9142072

[10] Madavi, K. B., &Karthick, P. V. (2021, November). Enhanced cloud security using cryptography and steganography techniques. *In 2021 International Conference on Disruptive Technologies for Multi-Disciplinary Research and Applications* (CENTCON) (Vol. 1, pp. 90-95). IEEE.https://doi.org/10.1109/CENTCON52345.2021.9687919

[11] Pant, V. K., Prakash, J., &Asthana, A. (2015, October). Three step data security model for cloud computing based on RSA and steganography. *In 2015 International Conference on Green Computing and Internet of Things (ICGCIoT)* (pp. 490-494). IEEE,https://doi.org/10.1109/ICGCIoT.2015.7380514

[12] Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing data security of cloud based lms. *Wireless Personal Communications*, 130(2), 1123-1139.https://doi.org/10.1007/s11277-023-10323-5

[13] Dudiki, N., Sangeetha, S., Manna, A., Pokhariyal, R., Mohanaprakash, T. A., &Srivastava, A. P. (2022, December). A Hybrid Cryptography Algorithm to Improve Cloud Computing Security. *In 2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 1020-1023). IEEE.https://doi.org/10.1109/IC3I56241.2022.10072437

[14] Abel, K. D., Misra, S., Agrawal, A., Maskeliunas, R., &Damasevicius, R. (2022). Data security using cryptography and steganography technique on the cloud. *In Computational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021* (pp. 475-481). Singapore: Springer Nature Singapore.https://doi.org/10.1007/978-981-16-8484-5_46

[15] Pandey, U., Rajput, M., & Singh, R. (2023, January). Role of Machine Learning in Resource Usages and Security Challenges for Cloud Computing: Survey. *In 2023 International Conference on Artificial Intelligence and Smart Communication (AISC)* (pp. 525-530). IEEE.https://doi.org/10.1109/AISC56616.2023.10085687

[16] Weng, C. Y., Weng, H. Y., & Huang, C. T. (2024). Expansion high payload imperceptible steganography using parameterized multilayer EMD with clock-adjustment model. EURASIP *Journal on Image and Video Processing*, 2024(1), 37.https://doi.org/10.1186/s13640-024-00653-0

[17] Zhanga, S., Xiaob, Y., Tianc, H., & Lid, X. (2025). A multi-image steganography: ISS. Cybersecurity, 8(1), 20.https://doi.org/10.1186/s42400-024-00333-6

[18] Gnanalakshmi, V., &Indumathi, G. (2023). A review on image steganographic techniques based on optimization algorithms for secret communication. *Multimedia Tools and Applications*, 82(28), 44245-44258.DOI:10.1007/s11042-023-15568-7

[19] Kumbhakar, D., Sanyal, K., &Karforma, S. (2023). An optimal and efficient data security technique through crypto-stegano for E-commerce. *Multimedia Tools and Applications*, 82(14), 21005-21018.https://doi.org/10.1007/s11042-023-14526-7

[20] Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., ...&Xue, M. (2023). Data hiding with deep learning: A survey unifying digital watermarking and steganography. *IEEE Transactions on Computational Social Systems*, 10(6), 2985-2999.https://doi.org/10.1109/TCSS.2023.3268950

[21] Pang, K. (2025). Provable Secure Steganography Based on Adaptive Dynamic Sampling. *arXiv preprint* arXiv:2504.12579.https://doi.org/10.48550/arXiv.2504.12579

[22] Omego, O., &Bosy, M. (2025). Multichannel Steganography: A Provably Secure Hybrid Steganographic Model for Secure Communication. *arXiv preprint* arXiv:2501.04511.https://doi.org/10.48550/arXiv.2501.04511

[23] Wang, Z., Byrnes, O., Wang, H., Sun, R., Ma, C., Chen, H., ...&Xue, M. (2023). Data hiding with deep learning: A survey unifying digital watermarking and steganography. *IEEE Transactions on Computational Social Systems*, 10(6), 2985-2999.https://doi.org/10.1109/TCSS.2023.3268950

[24] Butt, R., Tariq, N., Ashraf, M., Humayun, M., &Shaheen, M. (2025). Collaborative Defense: Federated Learning for Intrusion Detection Systems. In Federated Learning Systems: Towards Privacy-Preserving Distributed AI (pp. 147-165). Cham: Springer Nature Switzerland, https://doi.org/10.1007/978-3-031-78841-3_8

[25] Tariq, N., Alsirhani, A., Humayun, M., Alserhani, F., &Shaheen, M. (2024). A fog-edge-enabled intrusion detection system for smart grids. Journal of Cloud Computing, 13(1), 43 https://doi.org/10.1186/s13677-024-00609-9

[26] Saeed, F., Shaheen, M., Umer, T., Farooq, M.S. (2025). Employing Federated Learning for the Implication of Digital Twin. In: Afzal, M.K., Naeem, M., Ejaz, W. (eds) Digital Twins for Wireless Networks. Springer, Cham. https://doi.org/10.1007/978-3-031-73679-7_5

[27] Jawad, M., Iftikhar, S., Khan, R.A., Suleman, M.T., Umer, T., Shaheen, M. (2024). IoT-Driven Smart Housing: Strengthening Housing Society Automation Through Secure and Futuristic Networks. In: Rasheed, J., Abu-Mahfouz, A.M., Fahim, M. (eds) Forthcoming Networks and Sustainability in the AIoT Era. FoNeS-AIoT 2024. Lecture Notes in Networks and Systems, vol 1036. Springer, Cham. https://doi.org/10.1007/978-3-031-62881-8_25

[28] Ahmad, F., Najam, A., & Ahmed, Z. (2013). Image-based face detection and recognition:" state of the art".arXiv preprint arXiv:1302.6379 https://doi.org/10.48550/arXiv.1302.6379

[29] Shahzad, A., Chen, W., Shaheen, M., Zhang, Y., & Ahmad, F. (2024). A robust algorithm for authenticated health data access via blockchain and cloud computing. Plos one, 19(9), e0307039 https://doi.org/10.1371/journal.pone.0307039

[30] Ahmad, F., &Najam, A. (2012, October). Video-based face classification approach: A survey. In 2012 International Conference of Robotics and Artificial Intelligence (pp. 179-186). IEEE https://doi.org/10.1109/ICRAI.2012.6413396

[31] Tahir, S., Hafeez, Y., Humayun, M., Ahmad, F., Khan, M., &Shaheen, M. (2024). Harnessing hybrid deep learning approach for personalized retrieval in e-learning. PloS one, 19(11), e0308607 https://doi.org/10.1371/journal.pone.0308607

[32] Seth, A. (2025). Attack and Anomaly Detection in IoT Sensors Using Machine Learning Approaches. *Journal of Recent Innovations in Computer Science and Technology*, *2*(1), 16–27. https://doi.org/10.70454/JRICST.2025.20108

[33] Kumar, A., & Kumar, K. (2025). Facial Recognition and Object Detection using Machine learning. *Journal of Recent Innovations in Computer Science and Technology*, *2*(2), 39-48. https://doi.org/10.70454/JRICST.2025.20214

[34] Ahmad, N., Feroz, I., Ahmad, F. (2024). *Creating Synthetic Test Data by Generative Adversarial Networks (GANs) for Mobile Health (mHealth) Applications.* In: Rasheed, J., Abu-Mahfouz, A.M., Fahim, M. (eds) Forthcoming Networks and Sustainability in the AIoT Era. FoNeS-AIoT 2024. Lecture Notes in Networks and Systems, vol 1035. Springer, Cham. https://doi.org/10.1007/978-3-031-62871-9_25.

[35] Ahmad, F., Najam, A., & Ahmed, Z. (2013). *Image-based face detection and recognition: State of the art*. arXiv. https://doi.org/10.48550/arXiv.1302.6379

[36] Ahmad, F., &Najam, A. (2012). *Video-based face classification approach: A survey*. In *ICRAI 2012* (pp. 179–186). IEEE. https://doi.org/10.1109/ICRAI.2012.6413396