iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79174

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Hybrid Secure Data Concealment with Blockchain-Based Integrity Verification

P.Charan Satya Prakash[1], U.Raju[2], P.Venkateswarlu[3], Y.Asish Rahul[4], SK.Shakeel Ahmed[5]
[1, 23, 4, 5]*Student, Department of IT, VVIT, Guntur, A.P, Assistant Professor in VVIT, Guntur, A.P*

Abstract: ***This paper presents a hybrid secure data concealment system that enhances data security by integrating cryptography, steganography, and blockchain-based integrity verification. The system uses Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithms to encrypt sensitive data before embedding it into digital images using Least Significant Bit (LSB) steganography. To ensure data integrity, a SHA-256 hash of the concealed data is generated and stored in a blockchain-inspired append-only ledger. During verification, the extracted data is compared with the stored hash to detect tampering. Experimental results demonstrate that the proposed system ensures strong security, minimal image distortion, and reliable tamper detection. The system provides a secure and efficient solution for confidential data transmission.***
Keywords: Steganography, Cryptography, AES, RSA, SHA-256, Blockchain, Data Security

I. INTRODUCTION

With the rapid growth of digital communication, protecting sensitive data has become a big challenge. Traditional encryption methods keep data private but do not hide its existence, leaving it open to attacks.To tackle these issues, this paper suggests a combined secure data concealment system that mixes encryption, steganography, and blockchain-based verification. The system encrypts sensitive data, hides it in images, and checks its integrity using a blockchain-like ledger.This layered approach improves confidentiality, data concealment, and tamper detection. The system can be used in secure communication, banking, and military applications.

II. RELATED WORK

A. Steganography-Based Techniques

Steganography is a common way to hide secret information in digital files like pictures. These methods make data more private by hiding its existence. But they don't offer strong encryption or checks for integrity.

B. Cryptography-Based Techniques

Encryption is a way to protect data by using cryptographic algorithms like AES and RSA. These methods keep information private, but they don't hide it, which makes it easy to find.

C. Hashing and Integrity Verification

To make sure data is safe, hashing algorithms like SHA-256 create unique hash values for it. Changing any part of the data changes the hash value. But hashing by itself can't keep things private or hidden.

D. Blockchain-Based Verification

Blockchain technology provides a reliable ledger for storing data securely. It ensures that stored records cannot be changed. However, blockchain by itself does not offer data concealment.

E. Research Gap

From the analysis above, we see that most existing systems rely on individual techniques like steganography, cryptography, or hashing. However, these methods do not offer complete security.

III. METHODOLOGY

A. System Overview

The proposed system is designed as a hybrid security framework that integrates encryption, data hiding, and integrity verification techniques. By combining these multiple layers of security, the system ensures that data is transmitted in a highly secure and reliable manner, protecting it from unauthorized access and tampering.

B. System Workflow

The overall workflow of the proposed system begins with the user uploading an image and providing the confidential data to be secured. This data is first encrypted using a combination of AES and RSA algorithms to ensure a high level of security. The encrypted data is then embedded into the selected image using LSB (Least Significant Bit) steganography, allowing the information to be concealed without noticeable changes to the image. After embedding, a SHA-256 hash value is generated to create a unique digital fingerprint of the data. This hash is securely stored in a blockchain-based ledger to maintain data integrity and prevent unauthorized modifications. The secured image is then transmitted to the receiver. At the receiving end, the image is uploaded into the system for verification, where the hidden data is extracted and decrypted. The system then compares the newly generated hash value with the one stored in the ledger to detect any tampering. Based on this comparison, the system finally displays the result as either SAFE or TAMPERED, indicating whether the data has remained intact or has been altered.

C. Techniques Used

The proposed system incorporates several advanced techniques to ensure secure data handling and transmission. It utilizes AES and RSA algorithms for encrypting the data, providing strong protection against unauthorized access. To conceal the encrypted information within an image, LSB (Least Significant Bit) steganography is employed, allowing the data to remain hidden without affecting the visual quality of the image. Additionally, SHA-256 hashing is used to generate a unique digital fingerprint of the data, which helps in verifying its integrity. To further enhance security, a blockchain-based ledger is implemented to store the hash values, ensuring that any attempt to tamper with the data can be easily detected.

IV. SYSTEM ARCHITECTURE

A. Architecture Description

The proposed system consists of several interconnected modules that work together to ensure secure and reliable communication. Initially, the input module allows the user to provide both an image and confidential data. This data is then processed by the encryption module, where it is secured using AES and RSA algorithms.After encryption, the steganography module embeds the encrypted data into the image, effectively hiding it from unauthorized access. This makes the data less noticeable and adds an extra layer of security.In addition, the hashing module generates a SHA-256 hash value, which acts as a unique identifier for the data. This hash is stored in a blockchain-based ledger to maintain integrity and prevent any modifications.During the verification phase, the system extracts the hidden data from the image, decrypts it, and generates a new hash value. This hash is compared with the stored hash to check whether the data has been altered. If both values match, the data is considered safe; otherwise, it is marked as tampered.Overall, the system ensures data confidentiality, concealment, and integrity by combining multiple security techniques.

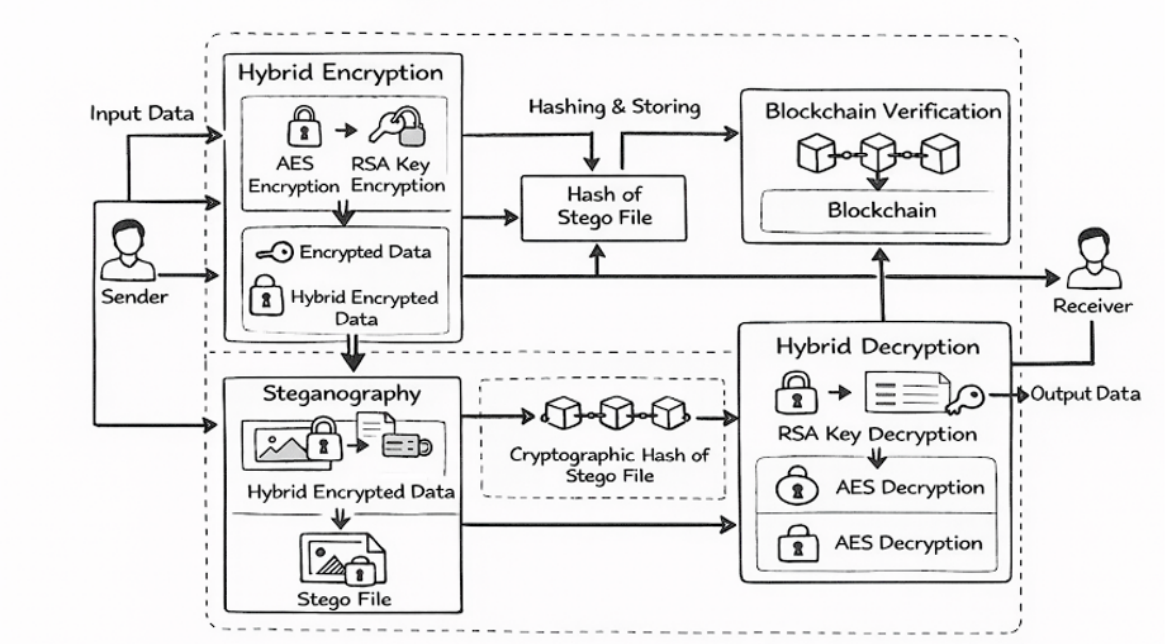


Fig.1: System Architecture

B. Modules of the System

Input Module: This module allows the user to upload the cover image along with the confidential data that needs to be secured.
Encryption Module: The collected data is protected using AES and RSA algorithms, ensuring strong encryption before further processing.
Steganography Module: The encrypted data is carefully embedded into the image using the LSB technique, making the hidden information unnoticeable.
Hash Generation Module: A SHA-256 hash value is generated to create a unique digital fingerprint of the data for integrity verification.
Blockchain Ledger: The generated hash is stored in a blockchain-based, append-only ledger, which helps prevent any unauthorized modification.
Verification Module: During verification, the system extracts and decrypts the hidden data, then compares hash values to detect any tampering.

V. RESULTS AND DISCUSSION

A. Implementation Results

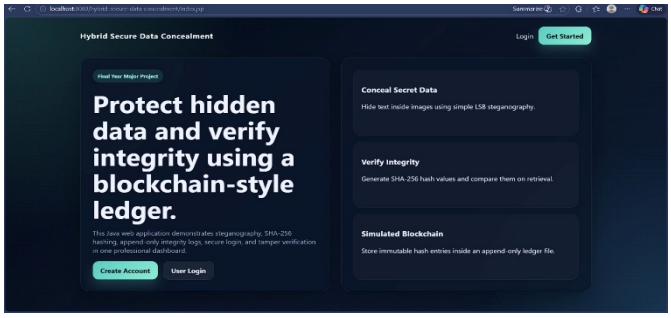


Fig. 2: Home Interface of Hybrid Secure Data Concealment System

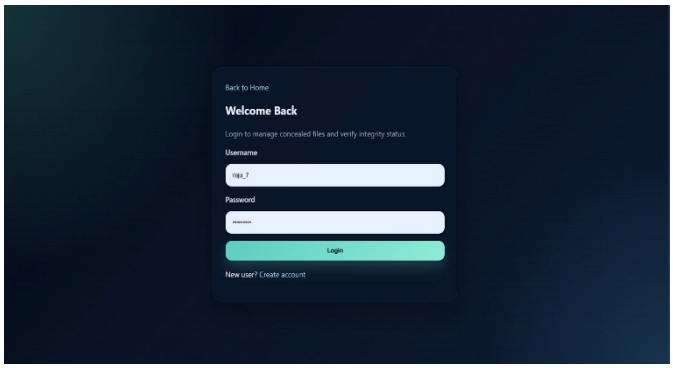


Fig. 3: User Login Interface

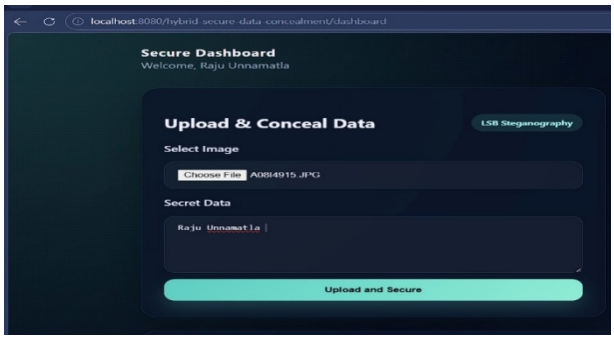


Fig. 4: Uploading Image and Entering Confidential Data

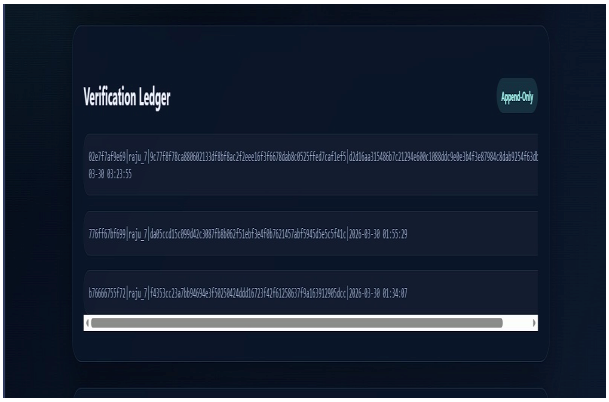


Fig. 5: Verification Ledger

B. Discussion

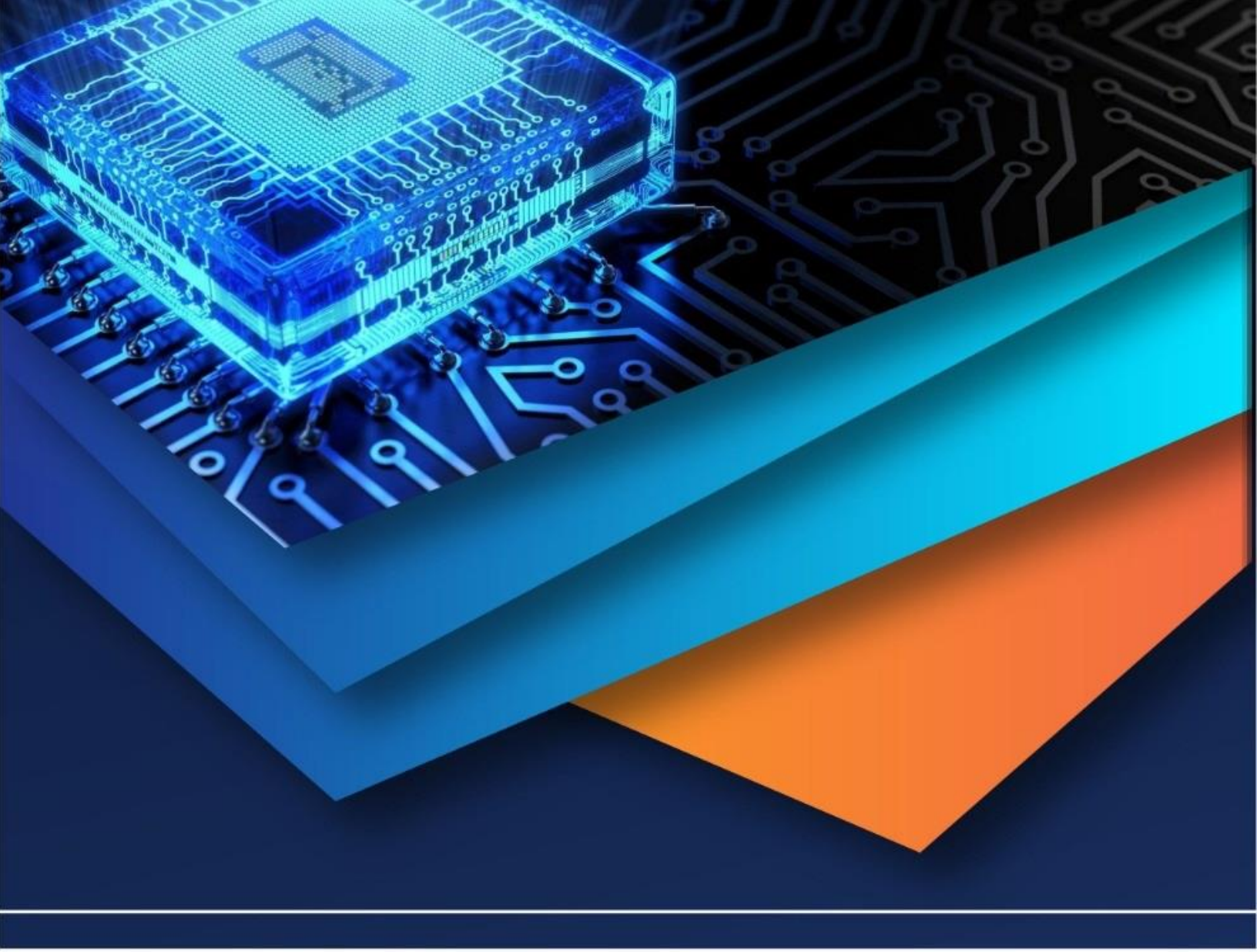
When compared to traditional approaches, the proposed hybrid model offers enhanced security by integrating encryption, data hiding, and blockchain-based verification. This combination not only strengthens data confidentiality but also ensures integrity by detecting any unauthorized changes. Furthermore, the use of a blockchain ledger prevents data manipulation, making the system more robust and trustworthy for secure communication.

VI. CONCLUSION

This paper presents a hybrid secure data concealment system that combines steganography, cryptography, and blockchain-based verification techniques. By integrating these methods, the system effectively ensures data confidentiality, hides sensitive information within images, and enables reliable detection of any tampering.The results show that the proposed approach performs efficiently and can be applied in real-world scenarios where secure and trustworthy communication is required.

REFERENCES

[1] N. F. Johnson, Z. Duric, and S. Jajodia, "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures," Kluwer Academic Publishers, 2001.
[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information Hiding - A Survey," Proceedings of the IEEE, vol. 87, no. 7, pp. 1062-1078, 1999.
[3] S. Katzenbeisser and F. A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking," Artech House, 2000.
[4] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32-44, 2003.
[5] J. Fridrich, "Steganography in Digital Media: Principles, Algorithms, and Applications," Cambridge University Press, 2009.
[6] W. Stallings, "Cryptography and Network Security: Principles and Practice," Pearson Education, 2017.
[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[8] R. C. Merkle, "A Digital Signature Based on a Conventional Encryption Function," in Proc. CRYPTO, pp. 369-378, 1987.
[9] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, "Bitcoin and Cryptocurrency Technologies," Princeton University Press, 2016.
[10] National Institute of Standards and Technology, "Secure Hash Standard (SHS)," FIPS PUB 180-4, 2015.
[11] D. Boneh and V. Shoup, "A Graduate Course in Applied Cryptography," 2020.
[12] Y. Zheng and X. Wang, "A Secure and Efficient Data Hiding Scheme for Digital Images," International Journal of Computer Applications, vol. 95, no. 1, pp. 20-26, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY