International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

Blockchain Integrated Secure Image Steganography using IPFS and Ethereum Sepolia Testnet

Dr. A. Radhika[1], D. Avinash[2], D. Sowjanya[3], K. Karthik[4], A. Venkat raj[5]
[1] Professor, SRK Institute of Technology, NTR, Andhra Pradesh, India
[2,3,4,5] Student, SRK Institute of Technology, NTR, Andhra Pradesh, India
Email ID: *Sai990750@gmail.com[1], Sowjanyadevireddy27@gmail.com[3]*

Abstract

The increasing use of digital communication has made it essential to maintain the confidentiality, integrity, and authenticity of sensitive information. Conventional image steganographic methods offer data hiding in digital images, but they fail to offer effective tamper proofing and secure ownership verification. To overcome these issues, this paper presents a Blockchain-Integrated Secure Image Steganography system using IPFS and Ethereum. In the proposed system, secret data is hidden within digital images using a Least Significant Bit (LSB) image steganographic method developed in Python. The stego images are then stored in the Inter Planetary File System (IPFS) for efficient and decentralized data storage. To ensure data integrity and secure access, the cryptographic hash values of the stego images and their corresponding IPFS Content Identifiers (CIDs) are securely stored on the Ethereum blockchain using smart contracts. The use of blockchain technology provides immutability, transparency, and tamper resistance, and IPFS provides decentralized storage without depending on centralized storage servers. The proposed system is validated to offer high image quality with negligible distortion and robust data security and traceability. This system is applicable for secure data sharing in confidential communication, digital forensics, and secure document transfer.

Keywords: Image Steganography, Blockchain, Ethereum, IPFS, Data Security, SHA-256

1. Introduction

In the current digital age, the rapid increase in multimedia data exchange over open networks has led to serious concerns about data security, privacy, and authenticity. Confidential documents, medical information, and private communications often contain sensitive data that is exchanged over open networks in digital form, making them susceptible to unauthorized access, interception, and modification. Traditional cryptographic methods aim to encrypt data but often neglect to hide the presence of communication, which can be a potential source of malicious attention. Steganography has been identified as an efficient method to improve data confidentiality by embedding secret information in digital media such as image, audio, or video files. Among various steganographic methods, image steganography is preferred because of the high redundancy and imperceptibility of digital images. However, traditional image steganographic methods have some serious drawbacks, including the absence of tamper-proofing, secure verification processes, and the need for centralized storage systems that are susceptible to single-point failures and data tampering. Blockchain technology offers a decentralized, immutable, and transparent ledger system that can overcome the above limitations. Ethereum, a popular blockchain platform, offers smart contract services that facilitate secure and automated data verification without the need for trusted third-party services. Concurrently, the Inter Planetary File System (IPFS) provides a distributed and content-addressable storage solution that guarantees efficient and robust storage of large multimedia files. The integration of blockchain and IPFS provides a robust infrastructure for secure data storage and verification. This paper presents a Blockchain-Integrated Secure Image Steganography system based on IPFS and Ethereum, where secret

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

information is hidden within digital images using a Least Significant Bit (LSB)-based steganographic method. The stego images are stored in IPFS, while their cryptographic hash values and IPFS storage identifiers are stored in the Ethereum blockchain using smart contracts. This method guarantees data integrity, traceability, and tamper-resistance while preserving high image quality. The proposed system overcomes the need for centralized servers and improves trust using decentralized verification. The system is applicable in scenarios demanding secure and stealthy data transmission, such as secure communication, digital forensics, intellectual property protection, and secure document exchange. Experimental results validate that the system efficiently balances security, performance, and imperceptibility, thus providing a practical solution for contemporary secure communication scenarios.

2. Literature Survey

Shahid Rahman et al. carried out a detailed survey on digital image steganographic methods, evaluating classical and contemporary approaches as well as performance metrics and security issues, but without introducing a novel implementation[1] Qin, Luo, Xiang, Tan, and Huang examined coverless image steganography, where the hidden data is embedded based on image characteristics rather than pixel manipulation, making it more resistant to detection but with limited data capacity[2] Chuang, Lin, Chen, and Shiu designed an RGB image steganography system based on adjacent mean embedding to counteract image distortion and improve stealthiness over traditional LSB-based steganography.[3] Gupta et al. presented a secure image steganography model by integrating cryptographic approaches such as AES and RSA algorithms with LSB steganography, ensuring double-layer data protection.[4] Sharma et al. designed a blockchain-based data integrity solution where data hashes are recorded on the blockchain for tamper-proof verification and robust data integrity.[5] K. Suresh et al. designed a decentralized storage solution based on IPFS for secure data transfer, overcoming the problem of single points of failure and improving file durability.[6] A. Patel and R. Mehta developed a blockchain-based secure image transmission system that checks image ownership and authenticity during online data transfer.[7] M. Reddy et al. proposed a hybrid security model that combines AES encryption with LSB-based steganography to improve the confidentiality of secure communication.[8] J. Thomas et al. discussed the concept of combining IPFS and blockchain technology to ensure secure data provenance, validation, and tamper-proof storage.[9] P. Kumar and N. Singh proposed a dual-security system that combines steganography and blockchain technology to ensure data secrecy and immutability, but with higher computational complexity.[10]

3. System Architecture

In this process, the sender embeds confidential information within a chosen cover image using LSB image steganography to produce a stego image. The stego image is then uploaded to IPFS, which produces a unique content identifier (CID). A SHA-256 hash of the stego image is computed, and the CID and hash are securely recorded on the Ethereum blockchain through a smart contract. On the receiving end, the CID is retrieved from the blockchain, and the stego image is downloaded from IPFS. The receiver computes a new hash of the downloaded image and compares it with the hash recorded on the blockchain. If the two hashes are equal, the image is declared unaltered, and the confidential information is successfully retrieved; otherwise, data tampering is indicated

4. Implementation

4.1.Interface

Interfaces are very important for the efficient operation of a software system as they help in the interaction of various components of the system and its users. In the proposed project, interfaces serve as the bridge between the frontend, backend services, blockchain network, and the decentralized storage systems like IPFS. The user interface is an interactive and user-friendly platform for the upload of images, embedding of secret information, and the retrieval of secured information. Application Programming Interfaces (APIs) help in the interaction of the frontend and backend services of the system, ensuring the smooth flow of data and its processing. Moreover, the smart contract interfaces help in the

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

interaction with the blockchain for the storage, verification, and validation of integrity. The interface for the integration with IPFS helps in the secure upload and retrieval of image files through their content identifiers

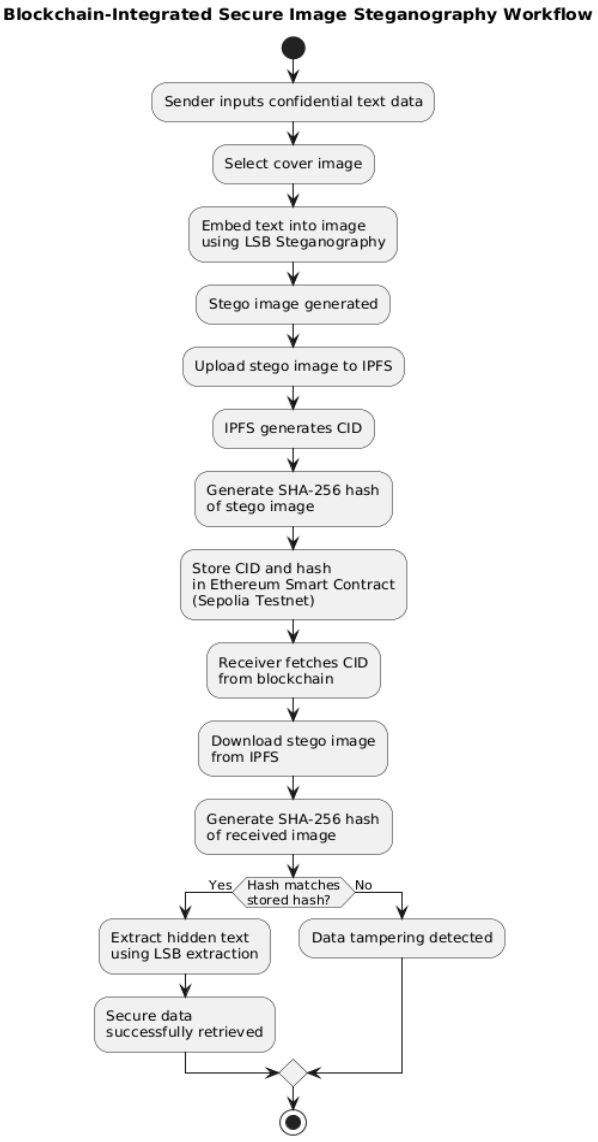

Figure 1 Flow Chart

4.2.Hide Data

In this interface, the user chooses a digital image, inputs secret text information, and optionally enters a password for added security. After entering the information, the system hides the secret information within the chosen digital image using image steganography methods. After the process is done, a confirmation message is shown to indicate that the information has been successfully hidden and stored securely. The interface also produces a unique image ID and IPFS hash, which is a representation of the stored steganographic image on the IPFS decentralized network. All this information is stored on the blockchain for added integrity, traceability, and tamper-proof verification. The interface also offers a step-by-step guide on how the user can securely transmit the stego image to the receiver. A download feature is also available for downloading the steganographic image, which contains the hidden secret information and can be verified or extracted later using the corresponding system modules.

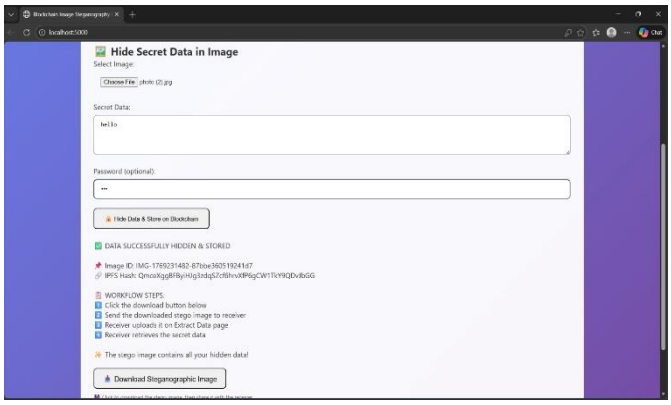

Figure 2 Hide Data

4.3.Extract Data

The Extract Secret Data interface allows authorized persons to extract the secret data from the steganographic image in a controlled and safe way. This interface allows two ways of extracting the secret data: either by uploading the received stego image or by using a distinct image ID. In the extraction process, the user uploads the steganographic image sent by the sender and also enters the password if encryption was used during the embedding process. After clicking on the extract button, the system analyzes the image and extracts the secret data embedded in the image using the reverse steganography algorithm. A confirmation message is shown after the completion of the extraction process, followed by the extracted secret message. This interface ensures confidentiality, authenticity, and accuracy of the data, thus completing the secure communication process

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

between the sender and the receiver.

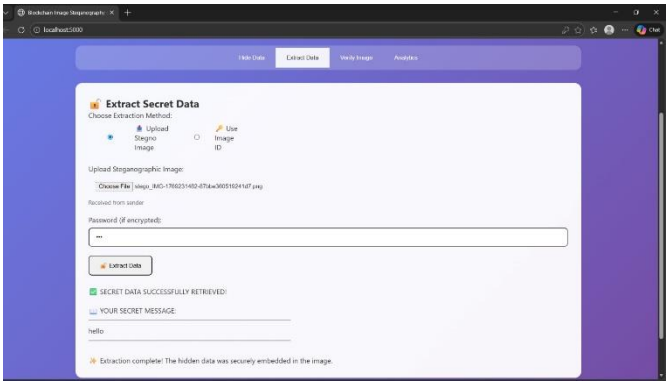

Figure 3 Extract Secret Data

4.4.Verify Image

The Verify Image Ownership interface is developed to verify the authenticity and ownership of the steganographic image through blockchain technology. In this interface, the user is required to enter a distinct image ID and its corresponding Ethereum address. Once the verification process is triggered, the system will access the Ethereum blockchain to verify the existing cryptographic hash and ownership information stored during the registration process of the image. If the entered information matches the information stored in the blockchain, a success message will be generated to confirm the successful verification of the image ownership. The interface is developed to provide transparency, non-repudiation, and tamper-proof verification of the image data to avoid any unauthorized modifications and misrepresentation of the image ownership.

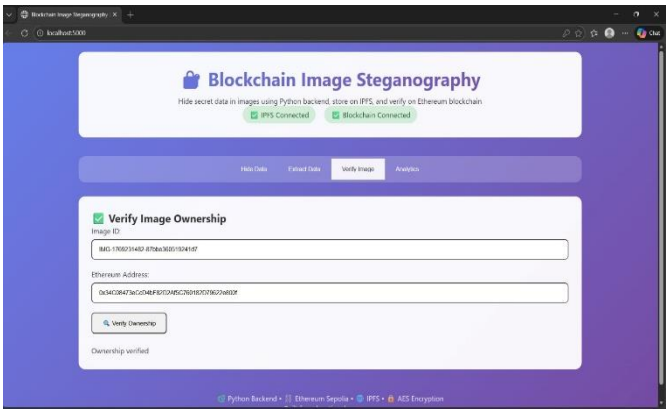

Figure 4 Blockchain Image

4.5.Analytics

The System Analytics interface is used for real-time monitoring and analysis of the overall health and usage of the Blockchain Image Steganography system. The interface shows the status of the critical system components, such as IPFS connectivity and blockchain availability, to ensure that the decentralized storage and verification functionality is working properly. The overall system health status and the last system check timestamp enable administrators to make informed judgments about the reliability and performance of the system. Furthermore, the analytics module enables users to fetch image statistics by submitting an Ethereum address, which promotes the transparent monitoring of all images linked to a particular user. The interface displays the total number of images and their respective unique image IDs, which are safely stored and indexed through blockchain information.

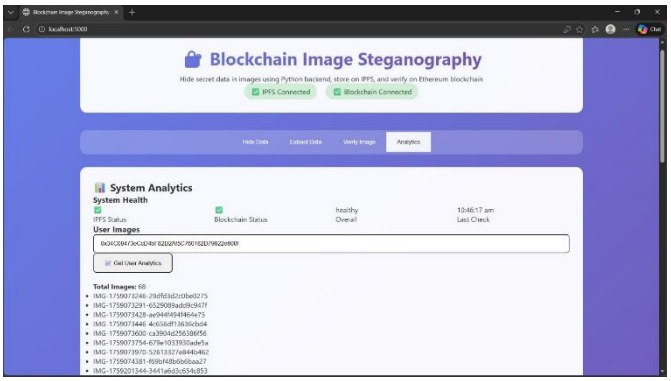

Figure 5 Block Chain Image 2

4.6.B.Technology

This approach applies image steganography based on the Least Significant Bit (LSB) method to securely embed confidential text messages into digital images. The cryptographic security is ensured by the application of the SHA-256 hashing algorithm, which is used to ensure data integrity and check for any possible tampering. The blockchain technology, in particular the Ethereum blockchain network running on the Sepolia test network, is applied in combination with smart contracts developed in Solidity to securely store and retrieve the IPFS content identifier (CID) and hash values. The stego images are stored in a decentralized manner using the Inter Planetary File

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

System (IPFS). Python is applied in the implementation of image processing and steganography operations, while Web3 technologies facilitate communication between the application and the blockchain.

4.7.C. Frontend Design

The frontend design of this system offers a simple and user-friendly interface that enables users to securely hide and retrieve data from images. The interface contains input fields for entering confidential text, a cover image selection field, and buttons for embedding and uploading tasks. The interface also shows key output results such as the generated IPFS CID, the status of the transaction from the blockchain, and the verification status. On the receiving side, the frontend design enables users to retrieve the CID from the blockchain, download the stego image, verify the image integrity, and extract the embedded message. The design is usually done using HTML, CSS, and JavaScript (or React.js) for responsiveness and smooth interaction with the backend and blockchain services.

4.8.D. Backend Services

The backend services of this system are responsible for the main processing and security tasks. These services are responsible for the image steganography process using the LSB method to hide and reveal the secret text from the image, calculating the SHA-256 hash value for image integrity, and handling file uploads and downloads from the IPFS. The backend services also communicate with the Ethereum blockchain using Web3 libraries to deploy and interact with smart contracts, storing and retrieving the IPFS CID and hash values. The backend services, which are implemented using Python, are a link between the frontend interface, IPFS storage, and the Ethereum blockchain.

4.9.V Deployement

The proposed system offers a secure and decentralized platform for secret communication using images by combining image steganography, cryptography, IPFS, and blockchain technology. The system provides confidentiality, integrity, authenticity, and non-repudiation of the hidden message during the communication process. First, the sender (Alice) chooses a cover image and a secret message to be sent securely. Prior to embedding the secret message into the cover image, the message is encrypted using cryptographic methods with the public key of the receiver, making it possible for only the receiver to decode the message. The encrypted message is then embedded into the cover image using an image steganography algorithm, generating a stego-image. The embedding operation conceals the existence of the message while preserving the image quality. After the stego-image is generated, it is uploaded to the InterPlanetary File System (IPFS). The IPFS is tasked with storing the image in a decentralized manner and generating a unique content identifier (hash) based on the image content. The hash is a unique identifier for the stored stego-image, ensuring content integrity since any change in the image content will result in a different hash value. The IPFS hash generated, along with other metadata such as image ID and timestamp, is then stored on the blockchain via a smart contract. The blockchain does not store the image but securely stores the hash and transaction information, ensuring immutability, traceability, and tamper-proof verification. This step ensures ownership verification and unauthorized modification of the stego-image is not possible. On the receiving side, Bob downloads the stego-image from the IPFS using the hash value received from the blockchain. Using the private key, the receiver decrypts the extracted data after completing the reverse steganographic extraction process. The system verifies the integrity of the received image by comparing the calculated hash value with the hash value stored in the blockchain. If the hash values are equal, the extraction process is successful, and the original secret message is received. In summary, this architecture offers a dual-layer security solution, where steganography is used to hide the existence of the data, cryptography is used for confidentiality, IPFS provides a decentralized and robust storage solution, and the blockchain provides integrity, verification of ownership, and non-repudiation of data. The combination of all these technologies

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

makes the system extremely secure, tamper-proof, and transparent, making it ideal for secure data transmission applications.

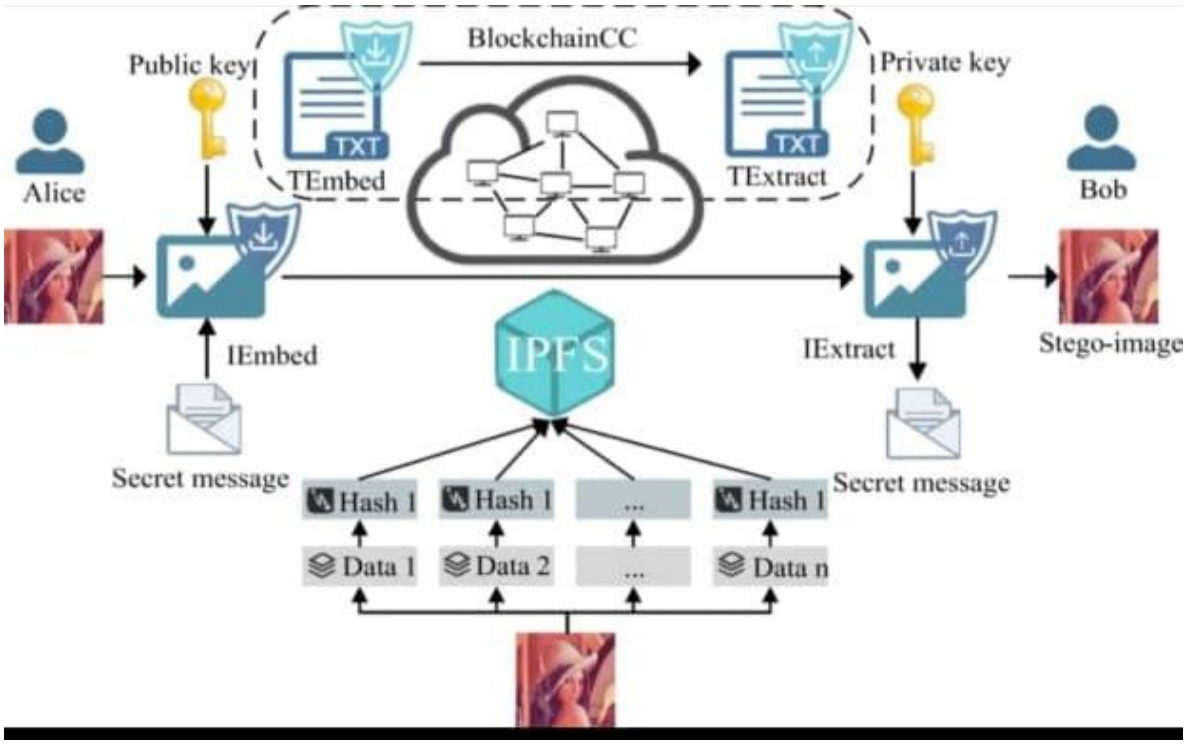

Figure 6 IPFS Process

Conclusion and Future Work

The future work of this system can concentrate on improving security, scalability, and usability. More advanced steganography algorithms and more secure encryption algorithms can be incorporated to further enhance the confidentiality and security of the data. The system can be developed to handle multiple file formats such as audio and video steganography, rather than being restricted to image steganography. Upgrading from a test network to a scalable mainnet or Layer-2 blockchain solution can help enhance performance and lower transaction costs. Moreover, incorporating access control systems, user authentication, and role-based authorization can further enhance security. Future improvements may also incorporate mobile app support, automated key management, and the utilization of artificial intelligence to identify steganalysis attacks.

Future Enhancements

The system can be developed to concentrate on enhancing security, efficiency, and practical usability. More advanced cryptographic methods like hybrid encryption can be incorporated along with LSB steganography for an additional layer of data security. The system can be developed to accommodate various media formats like audio and video steganography. The inclusion of Layer-2 blockchain solutions or sidechains can assist in lowering transaction fees. More advanced user authentication mechanisms, role-based access control, and secure key management can further enhance system security. In addition, the inclusion of AI-based steganalysis detection, mobile application support, and an interactive frontend dashboard can make the system more robust, scalable, and user-friendly for future development.

Conclusion

The proposed system is able to successfully combine image steganography with blockchain technology to ensure a secure and tamper-proof way of transmitting confidential data. By embedding confidential data into images using the LSB method and then storing them in a decentralized manner using IPFS, along

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2026.0039
e ISSN: 2584-2854
Volume: 04 Issue: 03
March 2026
Page No: 269 - 275

with verifying the integrity of the data using the Ethereum blockchain, the proposed system is able to ensure confidentiality, integrity, and transparency. The system is also able to ensure that the data is not tampered with by using cryptographic hashing.

Reference

[1]. Shahid Rahman, A Comprehensive Study of Digital Image Steganographic Techniques,2023, 10.1109/.
[2]. Qin, Luo, Xuyu Xiang, Tan, and Huang, Coverless Image Steganography, 2019, 10.1109/.
[3]. Chuang, Lin, Chen, Shiu, Steganography in RGB Images Using Adjacent Mean,2021, 10.1109/.
[4]. [4].Gupta et al, Secure File Sharing System Using Image Steganography and Cryptography Techniques,2023(Apr), 10.1109/.
[5]. Sharma et al, Blockchain Based Image Steganography, 2025,10.65521/.
[6]. K. Suresh et al Digital Image Steganography in the Spatial Domain Using Blockchain Technology, 2023.
[7]. A. Patel and R. Mehta, Designing a Secured Framework for the Steganography Process Using Blockchain and Machine Learning Technology,2023(Jan).
[8]. M. Reddy et al, Blockchain for Steganography, 2021.
[9]. [9]. J. Thomas et al, Secured Distributed Detection System Based on IPFS and Blockchain for Industrial Image and Video Data Security,2021,10.1016/.
[10]. P. Kumar and N. Singh, Steganograph Data Concealment in Images,2025,10.22214/.