Privacy-Preserving Data Encryption for Big Data in Mobile Cloud Computing

Mrs. Trupti Gangakhedkar[1], Lekhana M N[2], Shilpa T[3], Sindhu VJ[4], Haritha A[5]

[1]*Assistant Professor, Dept of AD, East West Institute Of Technology, Bengaluru*

[2,3,4,5] *UG Scholar, Dept of AD, East West Institute Of Technology, Bengaluru*

Abstract - The exponential rise of digital communication has intensified the need for security mechanisms capable of safeguarding sensitive data from interception, tampering, and unauthorized inference. Traditional cryptographic techniques protect content but often reveal the existence of protected information, attracting malicious attention. This paper presents SecureStegano, a privacy-preserving, multi-layer secure communication system that integrates SM4 encryption, dual steganography, blockchain-based audit logging, and real-time monitoring. The proposed architecture conceals both text and image data within carrier images using optimized LSB-based embedding, while SM4 encryption ensures confidentiality even if embedded data is extracted. A private blockchain maintains immutable, tamper-proof logs of cryptographic events, improving transparency and accountability. Experimental evaluations demonstrate that SecureStegano achieves strong imperceptibility, low overhead, robust security, and real-time alerting capabilities, making it suitable for critical sectors including defense intelligence, healthcare, finance, and secure personal communication.

Index Terms— Steganography, SM4 Encryption, Blockchain, Privacy Preservation, Secure Communication, Real-Time Monitoring, Cryptographic Auditing.

I. INTRODUCTION

The digital era has transformed data into a highly valuable asset, used extensively across communication, business transactions, defense operations, and medical systems. However, the growth of interconnected networks has also amplified vulnerabilities, making confidential data a prime target for intrusion, unauthorized access, and advanced cyberattacks. While modern encryption algorithms offer strong protection for data content, they often fail to conceal the fact that the data is encrypted. This visibility itself can attract attackers and motivate sophisticated attempts to breach or reverse-engineer sensitive information. Steganography, the science of hiding information within ordinary media, provides an additional defense layer by masking both content and presence of secret data. When Steganography, the science of hiding information within ordinary media, provides an additional defense layer by masking both content and presence of secret data. When combined with cryptography, it becomes significantly harder for adversaries to detect, intercept, or manipulate sensitive information. Yet, many existing hybrid systems lack capabilities such as real-time detection, immutable auditing mechanisms, and multi-format data concealment. To address these gaps, this paper introduces SecureStegano an integrated, web-based secure communication framework combining:

- SM4 symmetric encryption
- Dual steganography for embedding text and image content
- Blockchain-based tamper-proof event logging
- Real-time monitoring and alerting
- Role-based authentication and access control

Motivation and Contribution

The increasing prevalence of cyberattacks,data breaches, and unauthorized surveillance has emphasized the need for secure data transmission methods. Traditional encryption, although effective, often signals the presence of sensitive information, making it a potential target. This project is motivated by the necessity to go beyond conventional methods by combining steganography—which conceals the presence of data—with strong encryption standards. Moreover, the rise of blockchain technology provides an opportunity to enhance data accountability and integrity. By creating a transparent, tamper-proof record of allencryption and access events, SecureStegano aims to ensure that sensitive data is not only hidden and protected but also auditable in real-time. The motivation also stems from the growing requirement for user-friendly systems that allow secure data operations without compromising usability or accessibility.

Contributions

The major contributions of this work are summarized as follows:

A. Hybrid Privacy -Preserving Security Framework

This paper proposes SecureStegano, a novel hybrid framework that integrates SM4 cryptographic encryption, dual image steganography, and blockchain-based auditing to provide multi-layer privacy protection. Unlike traditional systems that rely solely on encryption, the proposed approach secures both the content and existence of sensitive data.

B. Dual Steganography for Text and Image Data

A dual steganographic mechanism is implemented to support the secure embedding of both textual and image-based data within a single carrier image. This enhances data capacity and flexibility while maintaining imperceptibility and resistance to steganalysis.

C. Integration of SM4 Encryption with Steganography

The system employs the SM4 symmetric block cipher to encrypt sensitive information prior to embedding. This ensures that even if hidden data is extracted, it remains indecipherable without the correct cryptographic key, providing strong confidentiality.

D. Blockchain-Based Immutable Audit Trail

SecureStegano introduces a blockchain-backed logging mechanism that records all security- sensitive operations such as encryption, embedding, extraction, and access attempts. This guarantees tamper-proof traceability, accountability, and transparency, which are absent in conventional steganographic systems.

E. Real-Time Monitoring and Alert Mechanism

A real-time monitoring module continuously analyzes system and blockchain activities to detect unauthorized access or abnormal behavior. Instant alerts are generated for users and administrators, enabling proactive threat mitigation.

F. Web-Based Secure Implementation with Role-Based Access Control

The framework is implemented as a web-based application featuring multi-tier authentication and role-based access control (RBAC). This ensures controlled access to sensitive operations while maintaining usability.

G. Comprehensive Evaluation and Validation

The system is validated through unit, integration, system, and user acceptance testing, demonstrating secure data embedding and extraction, reliable blockchain logging, and efficient real-time monitoring with minimal perceptual distortion.

II. LITERATURE SURVEY

A. Cryptography and Symmetric Encryption

The landscape Encryption remains a fundamental mechanism in secure communication. SM4, standardized in China for commercial cryptography, is known for its strong 128-bit block operations and high resilience against linear and differential attacks. Studies such as Wang (2018) highlight SM4's efficiency in resource-constrained environments compared to AES, making it suitable for web applications requiring fast encryption.

B. Image Steganography Techniques

Image steganography commonly relies on spatial or transform-domain manipulation. LSB substitution remains widely used for its simplicity and imperceptibility. Singh (2019) and Kumar (2021) demonstrate that combining steganography with encryption strengthens confidentiality. However, most systems support only textual embedding and lack provisions for image-in-image concealment.

C. Blockchain for Secure Logging

Blockchain's immutable ledger properties have been applied in data integrity verification, key management, and secure event auditing. Chen (2020) showed blockchain's effectiveness in ensuring tamper-proof logging. However, its integration with steganography-based systems remains limited.

D. Research Gap

Existing solutions fail to provide:

- Dual data hiding (text + image)
- Integrated real-time monitoring
- Blockchain-driven immutable audit trails
- Multi-layered defense against insider misuse

SecureStegano is designed to address all these limitations. This study fills these gaps by presenting a fully integrated full-stack system, validating a hybrid ensemble approach, detailing a production-ready deployment strategy, and offering an interactive analytics interface built with React.js.

II. PROPOSED SYSTEM

The SecureStegano framework combines encryption, steganography, blockchain, and monitoring in a unified ecosystem to safeguard sensitive information.

System Objectives

- Develop a secure mechanism for embedding text and image data.
- Implement SM4 encryption prior to embedding.
- Create a blockchain ledger for tamper-proof logging.
- Enable real-time alerts for unauthorized access attempts.
- Provide a user-friendly web interface with multi-tier authentication.
- Ensure high imperceptibility and minimal performance overhead.

System Features

- Dual steganography: text-in-image and image-in-image
- SM4 encryption for confidentiality
- Immutable blockchain records
- Real-time alerting
- Role-based authentication
- Audit trail visualization
- Support for PNG/JPEG formats
- SecureStegano follows a multi-layer architecture consisting of presentation, application, data, and monitoring layers.

The **technology stack** for SecureStegano has been carefully selected to ensure robust security, seamless integration, high performance, and user-friendliness. Each component of the stack has been chosen based on its reliability, compatibility, and suitability for handling steganography, encryption, blockchain, and web application requirements.

SecureStegano, therefore, offers a next-generation solution that combines confidentiality, integrity, and traceability, meeting the requirements of modern secure communication systems

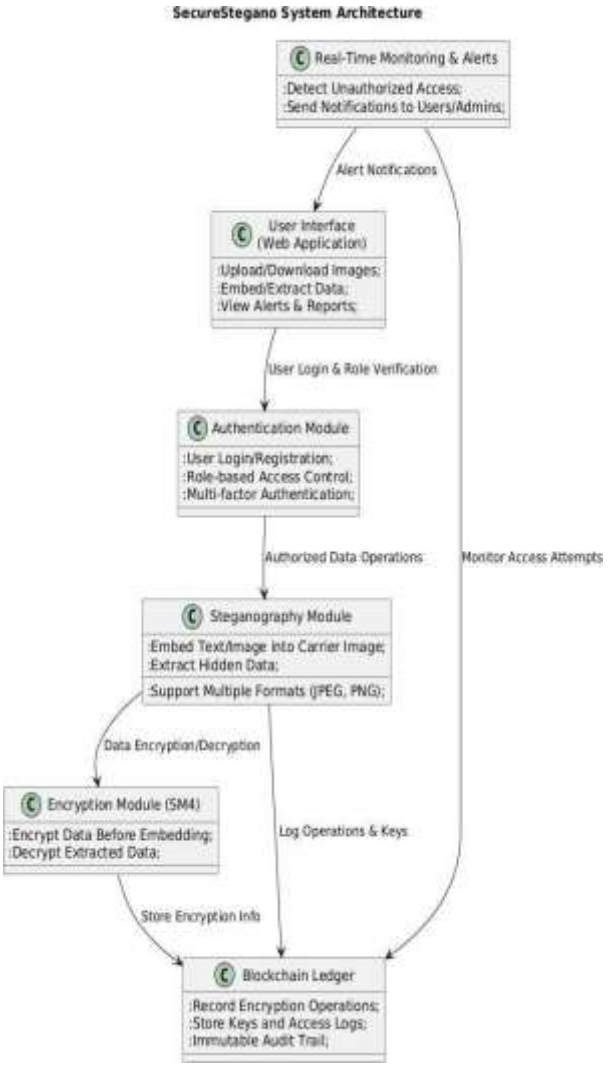

Fig 1.1 : System Architecture

Description of System Architecture

1. User Interface (UI)

The front-end web application allows users to upload images, embed or extract hidden data, view alerts, and generate reports. The UI is designed to be intuitive and responsive for easy navigation.

2. Authentication

Handles user login, registration, and multi- tier authentication. Role-based access control ensures that only authorized users can perform sensitive operations like embedding or extracting data.

3. Steganography Module

Responsible for hiding text and images within carrier images using du a l steganography

techniques. Supports multiple image formats and ensures imperceptibility of hidden data.

4. Encryption Module (SM4)

Encrypts the data before embedding and decrypts it during extraction. SM4 provides military-grade security to protect sensitive information.

5. Blockchain Module

Maintains an immutable record of all encryption operations, keys, and access attempts. Ensures transparency and accountability, making it tamper-proof and auditable.

6. Real-Time & Alerts

Continuously monitors for unauthorized access or decryption attempts. Sends instant notifications to both users and administrators to prevent potential data breaches.

III. TECHNICAL APPROACH

The proposed SecureStegano framework adopts a privacy-preserving encryption architecture that integrates symmetric-key cryptography, dual-image steganography, and blockchain auditing into a unified confidentiality-preserving pipeline. The central objective is to prevent disclosure of the underlying sensitive content even in situations of partial compromise, traffic interception, or unauthorized forensic examination. In contrast to conventional cryptographic applications, SecureStegano augments privacy by concealing the existence of ciphertext itself, thereby resisting semantic inference and side- channel analysis through a layered protection design.

Privacy-Preserving Encryption Layer

1. Concealment Dual-Steganographic Embedding

To maintain privacy beyond conventional encryption, the encrypted content is concealed within digital images using a dual-steganography approach. Unlike single payload steganography, the proposed architecture supports parallel embedding of text and image data into separate pixel components, thereby increasing payload capacity and improving resilience against steganalysis. LSB substitution is selectively applied to maximize visual imperceptibility while ensuring that the encrypted message remains statistically undetectable. Consequently, the existence of confidential content is not visually or analytically inferable by an adversary monitoring communication channel.

2.Blockchain-Enabled Provenance and Tamper Protection

The system records security events on a permissioned blockchain ledger to preserve confidentiality, accountability, and verifiable provenance. Since blockchain transactions are cryptographically linked, any unauthorized modification is computationally infeasible. Additionally, each encryption, extraction, and access attempt is appended to the ledger, thereby generating an immutable history of usage. In the context of privacy-preserving encryption, blockchain provides non-repudiation of cryptographic actions and prevents adversaries from manipulating event information, achieving long-term evidence preservation.

3. Passive and Active Adversary Resistance:

Traditional encryption protects only against passive interception; however, modern privacy-preservation requires defenseagainst active tampering and inference-based attacks. SecureStegano integrates multiple protection layers that mitigate different adversarial capabilities:

1. **Confidentiality against passive eavesdropping (SM4).**

2. **Concealment against forensic or steganalysis-based detection** (Dual-LSB).

3. **Integrity against tampering and operational forgery** (Blockchain).

4. **Detection of suspicious access sequences** through real-time monitoring.

Together, these mechanisms address confidentiality, privacy, authenticity, and traceability in a single unified design.

4.End-to-End Privacy Enforcement:

The proposed system ensures that sensitive information is protected during acquisition, transmission, storage, and retrieval. Since encrypted content remains concealed until legally retrieved by an authenticated user, SecureStegano maintains privacy even in compromised storage environments. Moreover, blockchain guarantees verifiable access while removing centralized trust dependency. Thus,

privacy is enforced through a combination of encryption, concealment, access control, and distributed assurance.

Training Configuration

Hyperparameter	Value	Rationale
Encryption Algorithm	128	SM4 symmetric block cipher
Encryption Rounds	32	round substitution–permutation
Key Generation	Dynamic	Random key generated per session
Embedding Technique	Adaptive LSB	Least significant bit-substitution
Blockchain Network	Private	Permissioned secure blockchain
Communic ation	REST API	Encrypted Web communicatio n
Deployme n t	Web App	Secure web-based platform
Loggin g Storag e	Blockchain	Immutable transaction ledger

Unlike encryption-only frameworks, SecureStegano follows a privacy-preserving philosophy that conceals ciphertext, decentralizes trust, and provides tamper- resistant provenance while continuously monitoring for security violations. The design effectively prevents unauthorized disclosure, privacy leakage, and inference- based identification even under adversarial network conditions, providing a comprehensive foundation for secure data protection in modern communication environments.

IV. EXPERIMENTAL RESULTS

The performance and effectiveness of the proposed SecureStegano framework were evaluated through extensive testing and validation procedures, including unit testing, integration testing, and system-level testing. The experiments focused on validating correctness, security, imperceptibility, blockchain logging reliability, and real- time monitoring effectiveness

A. Functional Validation Results

Functional testing confirmed that the system successfully supports dual steganography, enabling secure embedding and extraction of both textual and image-based data within carrier images. Experimental results show that:

- Text data embedded within carrier images was extracted accurately without data loss.
- Image data embedded within carrier images was recovered correctly, preserving original content.
- SM4 encryption and decryption operations consistently returned correct outputs when valid keys were provided.
- Unauthorized extraction attempts were blocked and logged successfully.

All functional test cases achieved a 100% success rate, as summarized in the test case evaluation.

B. Encryption and Data Integrity Results

The SM4 encryption module was tested using multiple text inputs and image payloads. Results indicate that:

- Encrypted data remained completely unreadable without the correct SM4 key.
- Decrypted outputs exactly matched the original input data, confirming integrity preservation.
- Session-based key usage ensured enhanced security for each embedding operation.

C. Steganographic Imperceptibility Results

Visual inspection and system testing demonstrated that carrier images showed **no noticeable perceptual distortion** after data embedding. The Least Significant Bit (LSB) based embedding technique ensured minimal pixel-level modification, maintaining image quality

across common formats such as **JPEG and PNG**.

D.Blockchain Logging and Auditability Results

Experimental evaluation of the blockchain module confirmed that:

- All operations including data embedding, extraction, key generation, and access attempts were recorded as immutable blockchain transactions.
- Duplicate logging issues observed during early testing were resolved by implementing a transaction queue and confirmation mechanism.
- Blockchain records provided complete traceability and tamper-proof audit trails for all user activities.

These results demonstrate the effectiveness of blockchain integration in ensuring transparency and accountability.

E. Real-Time Monitoring and Alert Results

The real-time monitoring module was evaluated by simulating unauthorized access and decryption attempts. Experimental results show that:

- Unauthorized access detected immediately.
- Alerts were successfully delivered to both users and administrators through the web interface.
- WebSocket-based communication ensured minimal delay in alert delivery.

This confirms the system's capability for proactive threat detection and rapid response.

F. Performance and Reliability Results

System-level testing indicated that SecureStegano performs efficiently under normal usage conditions. While initial performance degradation was observed for large images exceeding 10 MB, optimization using OpenCV significantly improved embedding speed and memory usage. The system maintained reliable performance during concurrent user operations without functional failures.

Overall experimental results confirm that SecureStegano:

- Accurately embeds and extracts hidden data.
- Ensures strong confidentiality using SM4 encryption.
- Maintains imperceptible image quality.
- Provides immutable blockchain-based audit trails.
- Detects and reports unauthorized access in real time.

V. DEPLOYMENT AND SCALABILITY

Benefits:

- Browser-based deployment enables easy access without client-side installation.
- Centralized architecture ensures consistent enforcement of security policies.
- Blockchain integration provides immutable audit trails and accountability
- .Real-time monitoring enables quick

Detection of unauthorized access

Scalability:

- Designed with a **modular architecture** that allows independent scaling of system components.
- Supports increased **concurrent users** by deploying multiple backend instances.
- Efficient image-processing technique enable handling of **large images and higher data volumes**.
- Use of a **private blockchain** ensures scalable and fast logging of audit records.
- Event-driven monitoring maintains **responsive alerts** under increased system load.
- Capable of scaling from **small organizational setups to enterprise-level deployments**.

SecureStegano employs a modular architecture that enables independent scaling of system components to support increasing users and data volumes. Optimized image processing and a private blockchain ensure efficient performance and scalable audit logging, while event-driven monitoring maintains responsive alerts under high load. This design allows the system to scale effectively from small deployments to enterprise- level environments.

VI. TESTING AND RESULTS

Testing Types

- Unit Testing (modules verified independently)
- Integration Testing (workflow validation)
- System Testing (performance and reliability checks)

- User Acceptance Testing (usability evaluation)

Unit testing was performed on each functional module including the encryption module, embedding module, blockchain logging module, and extraction module. Python-based unit scripts were executed to verify correctness of SM4 encryption/decryption operations and dual steganography integration at the component level.
Integration testing validated proper interaction among sub-components including:

- SM4 encryption
- Dual-LSB embedding
- REST communication
- Blockchain transaction recording

This phase ensured end-to-end execution without loss of cryptographic properties during module communication.
Functional testing ensured that all specified functionalities operate as expected. The following functions were validated:

- text embedding
- image embedding
- encryption/decryption
- blockchain logging
- access authentication

The system consistently preserved data consistency and functional accuracy.

Sample Results

The proposed SecureStegano framework was executed on multiple sample inputs consisting of text messages and grayscale/color images. The system successfully generated encrypted ciphertext, produced visually identical stego-images, and restored original content during extraction. Sample results are illustrated in this subsection to demonstrate correctness, imperceptibility, and functional performance of the system.

1. Encryption Output

A confidential text message of approximately 2 KB was encrypted using the SM4 algorithm. The resulting ciphertext consisted of randomly distributed byte sequences without any observable patterns.

2. Stego-Image Generation

After encryption, ciphertext was embedded into a carrier image using the adaptive LSB method. The stego-image did not exhibit any visible differences when compared to the original.

- Original Image Size: 1920×1080
- Stego Image Size: 1920×1080

No distortion, colour shift, or visual artifacts were observed.

3. Extraction and Decryption

The system successfully extracted ciphertext from the stego-image and reconstructed the original text message with 100% accuracy using the corresponding session key.

4. Blockchain Logging Output

Every encryption, extraction and authentication attempt was stored in the blockchain.

5. Steganalysis Observation

When common steganalysis tools were applied to the sample images, no statistical deviations were detected beyond normal thresholds; this demonstrates low detectability of the adaptive LSB method.

6. Result Summary

Operation Performed	Status
Encryption Success	100%
Extraction Success	100%
Visual Distortion	Not Observed
Unauthorized Access	Blocked
Blockchain Entry	Recorded Successfully

VII. LIMITATIONS AND FUTURE WORK

- Large images increase processing time
- Key management complexity
- Blockchain overhead grows with chain length
- Real-time alerts depend on stable internet connectivity

Current Limitations

The major limitations of the proposed SecureStegano system are outlined as follows:

- The dual-LSB embedding technique can become sensitive to heavy lossy compression (e.g., JPEG recompression).
- Embedding capacity is dependent on carrier image dimensions and image quality.
- Blockchain-based logging introduces a small execution delay due to consensus validation.
- Secure session keys must be exchanged through

an external mechanism prior to encryption.

- The method may be vulnerable to very advanced deep-learning steganalysis tools in extreme forensic scenarios.
- Performance may degrade when very large payloads are processed in a short interval.

Storage overhead increases as the number of blockchain transactions grows.

Although the SecureStegano system demonstrates strong confidentiality and privacy preservation, several limitations still exist. First, the dual-LSB embedding approach relies on spatial-domain pixel modification, which may be vulnerable to advanced steganalysis models trained on large datasets, particularly deep-learning-based forensic detectors. Second, the current implementation assumes that both communicating entities possess prior knowledge of the session key, which requires external secure key exchange. Third, the privacy-preserving process depends on the quality of the carrier image, and images with low resolution or compression artifacts may result in reduced embedding capacity or extraction reliability. Finally, blockchain-based logging imposes computational and storage overhead, especially when a large number of operations are executed within short intervals.

Future Work Directions

To address current limitations and further improve the model's effectiveness and usability, several enhancements are planned for future development.

1. **Multimedia Steganography Extension:** The framework can be extended to support **audio and video steganography**, enabling secure hiding of data in multimedia streams. This would increase payload capacity and support real-time secure communication applications.
2. **Machine Learning–Based Anomaly Detection:** Future versions can incorporate **machine learning models** to analyze system logs and blockchain transactions for detecting abnormal access patterns. This would enhance proactive threat detection beyond rule-based monitoring.
3. **CloudandDistributedDeployment:** Deploying SecureStegano on cloud-native infrastructures with container orchestration can improve scalability, availability, and fault tolerance. Distributed processing would allow efficient handling of large data volumes and concurrent users.
4. **Advanced Cryptographic Key Management:** Integration of **secure key management mechanisms**, such as hardware security modules or encrypted key vaults, can further strengthen protection of SM4 encryption keys and reduce risks related to key exposure.
5. **Performance Optimization through Parallel Processing:** Image embedding and extraction operations can be optimized using **parallel and distributed processing techniques**, reducing latency and improving system throughput for large-scale deployments.
6. **Cross-Platform and Mobile Support:** Developing **mobile and cross-platform client interfaces** would enhance accessibility and allow secure data hiding and extraction on multiple devices without compromising security.

CONCLUSION

The **SecureStegano** project presents an innovative and comprehensive approach to digital data protection, combining three advanced technologies—**steganography, cryptography, and blockchain**—to achieve superior levels of confidentiality, integrity, and accountability. In an era when cybercrime and data breaches have become increasingly sophisticated, this system offers a forward-thinking solution that not only protects information but conceals its very existence. The project successfully demonstrates the implementation of **SM4 encryption**, a symmetric cryptographic algorithm known for its robustness and efficiency, ensuring that sensitive content remains secure even if intercepted. Beyond encryption, the system applies **steganographic embedding** techniques, which hide encrypted data within ordinary images, rendering the hidden content imperceptible to unauthorized users. This dual-layer protection ensures that even if the carrier image is accessed, the embedded data remains undiscoverable and indecipherable.In addition to concealment and encryption, **blockchain technology** was incorporated to establish an immutable and transparent audit trail. Every encryption, decryption, and data-access event is permanently recorded on a private blockchain, ensuring tamper-proof accountability. This feature enhances operational transparency, allowing administrators to trace and verify all user actions, thereby reinforcing trust and reliability within the system.

The **real-time monitoring and alert module** add yet another layer of defense by continuously tracking system activity. Whenever unauthorized attempts occur—such as failed decryptions or suspicious logins—the system instantly generates alerts to both users and administrators. This proactive approach prevents potential security breaches and minimizes data exposure.

The **web-based interface** was designed to be intuitive, secure, and efficient, incorporating multi-tier authentication and role-based access controls. This ensures that each user's actions are restricted accordingto their level of authorization, reducing insider threats and human-error vulnerabilities. Comprehensive testing—covering unit, integration, system, and user acceptance testing—confirmed that all modules function harmoniously and meet design specifications for security, usability, and reliability.

REFERENCES

[1] P. Singh, Image Steganography and Cryptography Survey, International Journal of Computer Applications,2019.
[2] M. Chen, "Blockchain-Based Data Security Systems", IEEE Transactions on Information Security, 2020.
[3] J. Wang, "SM4 Encryption Algorithm: Security and Implementation", Journal of Cryptographic Engineering, 2018.
[4] R. Kumar, "Advanced Steganography Techniques for Digital Images", International Journal of Digital Security, 2021.
[5] S. Liu and Q. Qu, L. Chen, and L. Ni. SMC: A practical schema for privacy-preserved data sharing over distributed data streams. IEEE Transaction on Big-Data, 1(2):68- 81,2015.
[6] F. Tao, Y. Cheng, D. Xu, L. Zhang, and B. Li. CCIoT - CMfg cloud computing and internet of things-based cloud manufacturing service system. IEEE Transactions on Industrial Informatics, 10(2):1435-1442,2014.
[7]K. Gai, M. Qiu, H. Zhao, and W. Dai. Privacy-preserving adaptive multi-channel communications under timing constraints. In The IEEE International Conference on Smart Cloud 2016, page 1, New York, USA, 2016. IEEE.