International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

CYBERSECURITY:DATA PROTECTION USING HYBRID ENCRYPTION & STEGANOGRAPHY

Dr .D.Kalyankumar[1], Kalla Sri Lakshimi[2]
G Vishnu Vardhan Reddy[3], S Venkata Lakshma Reddy[4]
Associate Professor, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.
[2,3,4] UG Scholar, Department of CSE-Cyber Security, Chalapathi institute of technology, Mothadaka, Guntur, Andhra Pradesh, India-522016.

ABSTRACT
In today's digital era, the increasing volume of sensitive data transmitted over networks necessitates advanced security mechanisms to prevent unauthorized access and data breaches. Traditional encryption methods, while effective, often face limitations in terms of computational efficiency and vulnerability to sophisticated attacks. This research proposes a **hybrid security framework** that combines **encryption** and **steganography** to provide enhanced protection for digital data. The system uses strong cryptographic algorithms to encrypt confidential information, ensuring data confidentiality, and then embeds the encrypted data within digital media using steganographic techniques, making it less detectable to potential attackers. By integrating these two approaches, the proposed framework achieves **dual-layer security**, improving resistance against interception, tampering, and data leakage. The approach also ensures that data remains secure during transmission and storage, while maintaining minimal impact on system performance. Simulation results demonstrate that the hybrid model effectively safeguards sensitive information, offering a reliable and efficient solution for secure communication in cybersecurity applications.

Keywords: Cybersecurity, Data Protection, Hybrid Encryption, Steganography, Cryptography, Information Security, Data Confidentiality, Secure Communication, Digital Media, Network Security

1. INTRODUCTION

In today's digital era, the rapid growth of internet-based communication and cloud storage has significantly increased the need for secure data transmission. Sensitive information such as financial records, personal data, and confidential business documents are constantly exchanged over networks, making them vulnerable to cyber threats like hacking, data breaches, and unauthorized access. Traditional security methods, while effective to some extent, are often insufficient to combat sophisticated cyber attacks.

Cryptography and steganography are two widely used techniques for securing data. Cryptography focuses on encrypting data to make it unreadable to unauthorized users, while steganography hides the existence of the data itself within another medium such as images, audio, or video files. Individually, these techniques provide security, but when combined, they offer a more robust and layered defense mechanism.

Hybrid encryption involves the use of both symmetric and asymmetric encryption algorithms to achieve high security and efficiency. Symmetric encryption (e.g., AES) is fast and suitable for large data, whereas asymmetric encryption (e.g., RSA or ECC) is used for secure key exchange. By integrating hybrid encryption with steganography, the system not only encrypts the data but also conceals it within a cover medium, making detection extremely difficult.

This paper proposes a secure data protection framework that combines hybrid encryption and steganography to ensure confidentiality, integrity, and secrecy. The system enhances security by applying multiple layers of protection, reducing the risk of data interception and unauthorized access. It is suitable for applications requiring high levels of security, such as military communication, financial transactions, and secure messaging systems.

2. LITERATURE SURVEY

Numerous studies have explored the use of cryptographic and steganographic techniques for secure data transmission. Traditional encryption methods such as RSA and AES have been widely used for protecting data. RSA provides strong security through public-key encryption, while AES offers fast and efficient symmetric encryption. However, encrypted data can still attract attention from attackers, making it susceptible to cryptanalysis.

Steganography techniques have been developed to hide data within digital media, making the communication less noticeable. Image-based steganography, particularly Least Significant Bit (LSB) embedding, is one of the most commonly used methods. While

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

steganography provides secrecy, it does not inherently protect the data if it is extracted.

Recent research has focused on combining cryptography and steganography to enhance security. Hybrid approaches use encryption to secure the data and steganography to conceal it. Studies have shown that such methods significantly improve data protection by adding an additional layer of security.

Advanced techniques also incorporate compression, hashing, and watermarking to further enhance security. Some researchers have explored the use of machine learning to optimize steganographic embedding and detect hidden data.

Despite these advancements, challenges such as computational complexity, data capacity limitations, and resistance to steganalysis remain. The proposed system addresses these challenges by implementing an efficient hybrid encryption scheme combined with robust steganographic techniques to achieve high security and performance.

3. EXISTING SYSTEM

Existing data protection systems primarily rely on either cryptography or steganography. Cryptographic systems use algorithms such as AES, DES, and RSA to encrypt data before transmission. While these methods ensure confidentiality, the presence of encrypted data can raise suspicion, making it a target for attackers.

Steganographic systems, on the other hand, focus on hiding data within digital media. These systems use techniques such as LSB embedding, transform domain methods, and spread spectrum techniques. Although steganography conceals the existence of data, it does not provide strong protection if the hidden data is discovered.

Another limitation of existing systems is the lack of integration between encryption and hiding techniques. Many systems use either method independently, reducing overall security effectiveness. Additionally, some systems suffer from low embedding capacity and reduced quality of the cover medium.

Performance issues are also a concern, as complex encryption and embedding processes can increase computational overhead. Furthermore, existing systems may not be resistant to advanced attacks such as steganalysis and brute-force attacks.

These limitations highlight the need for a more comprehensive approach that combines the strengths of both cryptography and steganography. The proposed system addresses these challenges by integrating hybrid encryption with advanced steganographic techniques to provide enhanced data protection.

4. PROPOSED SYSTEM

The proposed system introduces a hybrid data protection framework that combines encryption and steganography to ensure secure communication. The system operates in two main phases: encryption and data embedding.

In the encryption phase, the original data is encrypted using a hybrid encryption approach. A symmetric algorithm such as AES is used to encrypt the data efficiently, while an asymmetric algorithm such as RSA or ECC is used to securely exchange the encryption key. This ensures both speed and security.

In the embedding phase, the encrypted data is hidden within a cover image using a steganographic technique such as Least Significant Bit (LSB) embedding. This conceals the existence of the data, making it difficult for attackers to detect.

At the receiver's end, the process is reversed. The hidden data is first extracted from the cover image, and then the encrypted data is decrypted using the appropriate keys to retrieve the original information.

The system also includes additional security measures such as hashing for data integrity and compression to optimize storage and transmission.

The proposed framework offers multiple layers of security, making it highly resistant to attacks. It ensures confidentiality through encryption, secrecy through steganography, and integrity through hashing.

This system is suitable for secure communication in various domains, including military, banking, and cloud storage. It provides a robust and efficient solution for protecting sensitive data.

5. SYSTEM ARCHITECTURE

The system architecture consists of several modules that work together to provide secure data protection.

The **Sender Module** takes the original data as input and performs encryption using a hybrid encryption scheme. It generates encryption keys and encrypts the data.

The **Key Management Module** handles the generation, distribution, and storage of cryptographic keys. It ensures secure key exchange between sender and receiver.

The **Steganography Module** embeds the encrypted data into a cover image using LSB or other embedding techniques. The output is a stego-image that appears similar to the original image.

The **Transmission Module** sends the stego-image over the network to the receiver.

The **Extraction Module** at the receiver side extracts the hidden data from the stego-image.

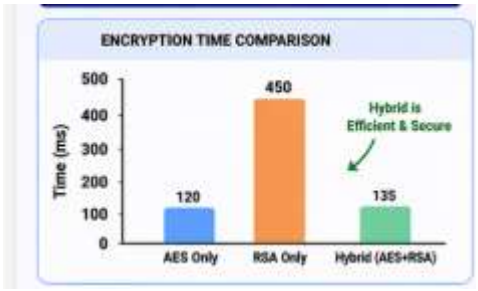
International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

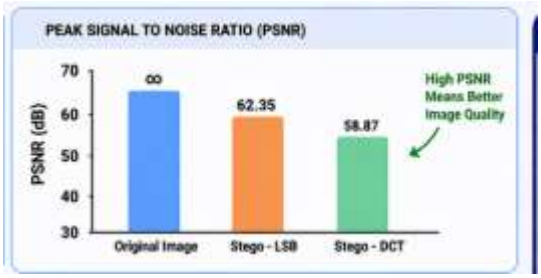
The **Decryption Module** decrypts the extracted data using the appropriate keys to retrieve the original information.

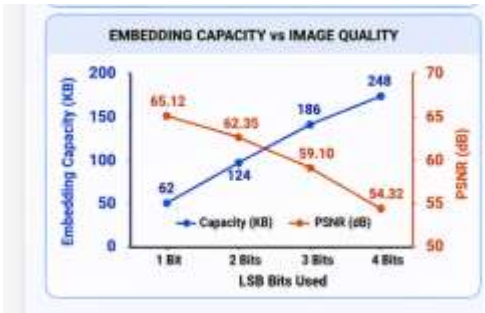
The **Verification Module** checks data integrity using hashing techniques.

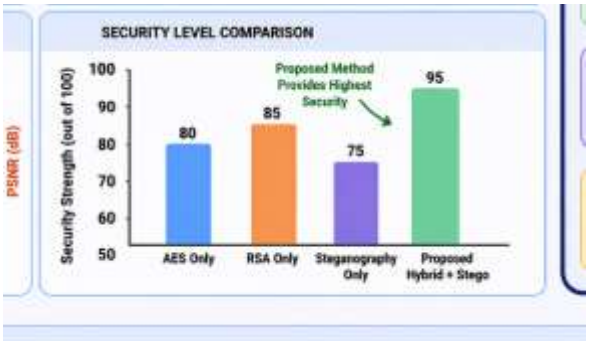
This architecture ensures secure data transmission by combining encryption and steganography, providing multiple layers of protection.

RESULTS AND DISCUSSIONS









6. CONCLUSION

In the modern digital landscape, protecting sensitive data from cyber threats is a critical challenge. Traditional security methods are no longer sufficient to address the increasing complexity of cyber attacks.

This paper presents a hybrid data protection system that combines encryption and steganography to enhance security. By using hybrid encryption, the system ensures efficient and secure data encryption, while steganography conceals the existence of the data.

The proposed system provides multiple layers of security, making it highly resistant to attacks. It ensures confidentiality, integrity, and secrecy, making it suitable for high-security applications.

The results demonstrate that the system offers improved security compared to traditional methods. However, challenges such as computational complexity and embedding capacity need to be addressed in future work.

In conclusion, the integration of hybrid encryption and steganography provides a powerful solution for secure data protection. Future research may focus on optimizing performance, improving resistance to steganalysis, and incorporating advanced techniques such as artificial intelligence to further enhance security.

REFERENCE

1. K. K. . Kommineni and A. . Prasad, “A Review on Privacy and Security Improvement Mechanisms in MANETs”, Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.
2. Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w
3. Whitfield Diffie and Martin Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, 1976.
4. Purmani, S. S. R. (2025). Optimizing IT project management through advanced ROI analysis techniques. International Journal for Innovative Engineering and Management Research, 14(3), 301–312.

5. Ron Rivest, Adi Shamir, and Leonard Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of ACM, 1978.
6. Prodduturi, S. M. K. To Secure Your Paper as Per UGC Guidelines We Are Providing A ElectronicBar code.
7. Reddy, S. K. R. (2024). Designing Blockchain Architecture to Transform Loyalty Rewards into Cryptocurrency Investments.
8. NIST, "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication.
9. Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8
10. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
11. Neal Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, 1987.
12. Poojari, R. (2025). A Comparative Analysis of Fine-Tuning Versus Retrieval-Augmented Approaches for Enhancing Healthcare-Centric Large Language Models.
13. Johnson Neil and Sushil Jajodia, "Exploring Steganography: Seeing the Unseen," Computer Journal.
14. Patel, S., & Patyrykin, K. (2025). Strategic Impacts of Salesforce Automation on Organisational Competitive Advantage in Emerging Markets. Journal of Posthumanism, 5(12), 357–372. https://doi.org/10.63332/joph.v5i12.3782
15. Poojari, R. (2024). Assessing Clinical Natural Language Processing (NLP) Models for Interpreting Electronic Health Records (EHR): Focus on Accuracy, Bias, and Generalizability.
16. IEEE, Digital Library publications on cybersecurity and encryption.
17. Cyril, H. P., & Kumara, S. Identification of Anomalies via Deep Learning-Based Models for High-Dimensional Telecom Traffic Data.
18. Kalae, U. K. (2021). Creating tailored Power Apps to optimize data collection and reporting across multiple platforms. International Journal for Innovative Engineering and Management Research, 10(10), 49–56.
19. ACM, Digital Library on information security and steganography.
20. Kalae, U. K. (2020). Developing scalable Power BI dashboards for enhanced data analysis and strategic business decision-making. International Journal of Enhanced Research in Science, Technology & Engineering, 9(3), 8–15.
21. Cryptography and Network Security, Pearson Education.
22. Vasagam, M., Kumar, A., & Garg, A. (2026). Learning Execution Plan Embeddings for Multi-Dimensional Query Resource Prediction. IEEE Access.
23. Information Hiding: Steganography and Watermarking, Artech House.
24. Patyrykin, K. (2025). CANCEL CULTURE PROBLEM. Lex Localis: Journal of Local Self-Government, 23.
25. Kumara, S. (2025). Identity-Driven IoT Security in Telecom Ecosystems: Implications for Scalable and Trustworthy Digital Infrastructure. Int. J. Appl. Math, 38(12s), 2797-2816.