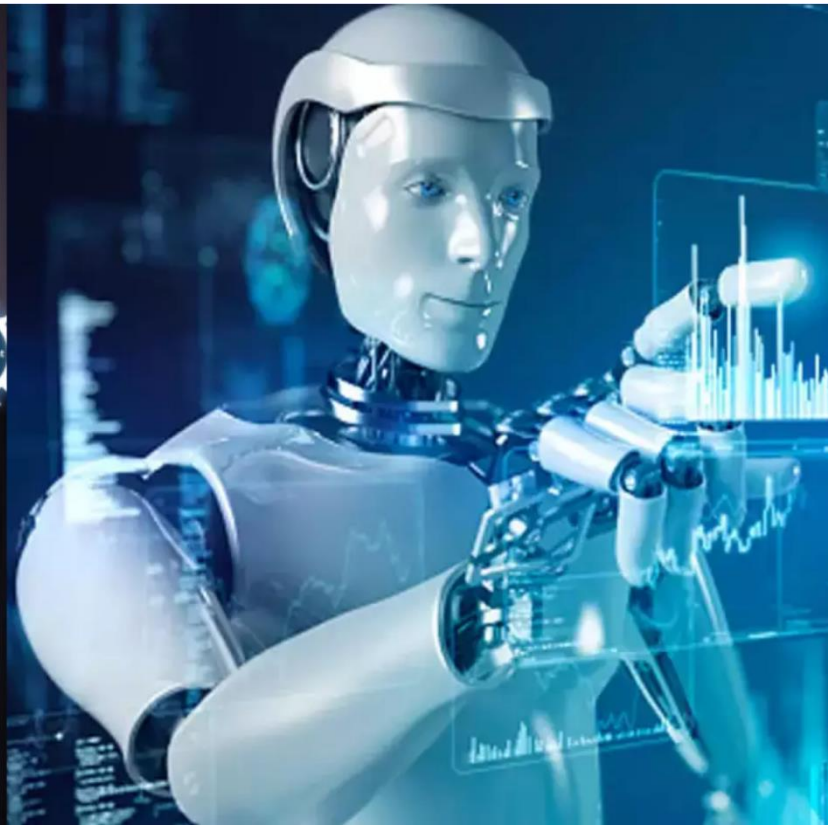
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 4, April 2025

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404048|

Enhancing Data Security with Cryptography, Steganography and File Encryption

K Anuranjani [1], Gande Harishankar[2], Pendyala Ganesh[3], Gaddam Ganesh[4], Ganapathiraju Dattaraj Varma[5]

Assistant Professor, Department of CSE Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

B. Tech Students, Bharath Institute of Higher Education and Research, Selaiyur, Chennai, Tamil Nadu, India

ABSTRACT: In a world where data breaches and cyber attacks are becoming more common, maintaining strong data security is now an essential priority. This project seeks to examine an integrated method for protecting sensitive information through the combination of cryptography, steganography, and file encryption. Cryptography offers a base level of security by encrypting data into an unreadable form, which can be read only by trusted individuals who have the proper decryption key. Steganography adds to this by hiding the fact that the data exists, inserting it into harmless carriers like images or audio files to avoid detection. The system proposed here provides a flexible solution for secure storage and communication, with possible uses in areas demanding high privacy levels, including finance, healthcare, and national security

KEYWORDS—Data Security, Cyber Threats, Data Breaches, Cryptography, Steganography, File Encryption, Decryption Key, Sensitive Information, Secure Communication, Storage, Privacy, Finance, Healthcare, National Security

I. INTRODUCTION

The speed of data exchange and storage of sensitive data in the current digital environment has placed data security in the center of attention for all kinds of businesses, ranging from healthcare and finance to national security. With cyber threats evolving at a more complex level from brute-force attacks to quantum computing-based vulnerabilities, mere standalone encryption cannot be an adequate security mechanism. Encryption, though efficient in protecting information, has a basic flaw: the fact that there is encrypted information will draw the attention of cybercriminals. Furthermore, the vulnerability of exposing encryption keys renders even highly secured systems vulnerable to attacks. Counteracting these, there is a critical need for a next-generation security model that not only guarantees data confidentiality but also stealthiness during transmission and storage.

This project presents an all-around security model that includes cryptography, steganography, and file encryption to improve the protection of data. Cryptography protects data through encrypting plaintext into unreadable ciphertext using powerful encryption algorithms such as AES (Advanced Encryption Standard). Nevertheless, encryption does not stop an attacker from identifying encrypted files and making attempts to decrypt them. In addition to protecting sensitive information, steganography is integrated to hide encrypted data inside normal media files, like pictures or sound, so that the existence of the data itself remains hidden. Last but not least, file-level encryption serves as a second line of defense, ensuring that no unauthorized access occurs even if the hidden file is found.

Besides these benefits, challenges persist in effectively implementing such a multi-layered security system. Computational overhead, key management, and retrieval accuracy are the essential factors that affect the efficiency of this system. These are addressed through the optimization of encryption and steganographic embedding methods to reduce latency in processing while ensuring maximum security and stealth. The solution is user-centered, scalable, and flexible, supporting both personal and enterprise security requirements.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404048|

The goal of this research is to contribute to the continuous evolution of sophisticated data protection methods through the introduction of a safe, multi-layered encryption and cover system that provides better protection against contemporary cyber attacks. The efficacy of the proposed system is assessed by conducting simulations and security analysis, proving it as an effective means to protect sensitive data from unauthorized access, eavesdropping, and detectability.

The remainder of this paper is organized as follows: Section II is a literature survey of current encryption and steganography methods. Section III outlines the proposed system's methodology, including encryption algorithms, steganographic embedding, and security analysis. Section IV explains experimental results and system performance. Lastly, Section V concludes with major findings and suggestions for future work.

II. LITERATURE REVIEW

In the future, the project can further be improved with the addition of quantum cryptography methods, which take advantage of quantum mechanics principles to develop encryption methods that are theoretically unbreakable, thus achieving an unprecedented level of security capable of resisting even the most powerful computational attacks, making it very suitable for use in national security, financial transactions, and highly confidential communications where common encryption methods can eventually be broken by the high rate of increase in computing power. With the incorporation of *machine learning (ML) and artificial intelligence (AI) algorithms, this project can be enhanced to autonomously identify security vulnerabilities, optimize steganographic embedding and encryption methods, and dynamically evolve to counter new-emerging cybersecurity threats*, keeping the system resistant to new-emerging hacking techniques and unauthorized access attempts while maintaining minimal computational overhead and increased real-time secure communication efficiency.

The definition of real-time data security can be further broadened by deploying this project in live video streaming, voice-over-IP (VoIP) calls, and secure online messaging services, where steganographically hidden encrypted messages may be embedded in audio or video frames for undetectable and extremely secure communication of sensitive information on global communications networks, which will be highly useful for intelligence organizations, corporate communications, as well as diplomatic negotiations where confidentiality is the topmost concern.

With the growing use of blockchain technology, this project can be implemented in decentralized systems where data can be safely stored and transferred over tamper-proof and immutable distributed ledgers so that sensitive information is safe from cyber attacks, unauthorized changes, and data tampering, thus meeting the rising demands around secure data exchange, identity authentication, and digital asset securityin sectors like finance, healthcare, and e-governance.
With advancements in cloud computing and Internet of Things (IoT) technologies, this project can be used to offer end-to-end encrypted and steganographically protected data storage and transmission solutions, allowing highly confidential data to be concealed in digital media files and transmitted securely over cloud-based infrastructures and networked IoT devices, which would immensely lower the risk of **cyber espionage, data breaches, and unauthorized surveillance, thus providing a **highly scalable and future-proof solution to data security in smart cities, industrial automation, and critical infrastructure management.

provide me with more material as example Post-Quantum Cryptography Integration As quantum computing continues to evolve, classical cryptographic techniques like RSA and ECC will increasingly be at risk. Subsequent versions of this project can incorporate post-quantum cryptography (PQC), which uses lattice-based, hash-based, and multivariate polynomial cryptographic methods to create encryption schemes that are quantum-resistant. This would provide long-term security for sensitive information, especially in use cases like government communications, military missions, and protection of critical infrastructure, where confidentiality is to be ensured beyond the quantum age.guarantee. A low-overhead processing security model with strong privacy features is in great demand.
Federated learning would enable AI models to be trained jointly across devices, making adaptive security features possible to combat new cyber threats while maintaining user privacy.

This would be especially beneficial in secure healthcare data exchange, edge computing, and smart contracts environments, where local security policies have to be dynamically updated without exposing sensitive data. Homomorphic Encryption for Secure Data Processing To provide added security to cloud environments, this project

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404048|

can integrate homomorphic encryption, which allows data to be computed on while it is still encrypted, so that sensitive data is kept secure during computations. This method would be extremely useful in financial analysis, private business calculations, and privacy-preserving AI models, where companies must compute sensitive data without sharing it with external servers or third parties.

Multi-Factor Biometric Security
For enhanced security against authentication threats, this project can incorporate multi-factor biometric encryption methods that blend fingerprint, retina scan, voice recognition, and behavioral biometrics for enhanced access controls. This would be particularly useful for high-security sectors like defense, preventing corporate espionage, and entry to classified research so that even if physical encryption keys are threatened, unauthorized access is still virtually non-feasible.

Secure Supply Chain Communication and IoT Protection
With the increasing connectivity of supply chain networks and IoT environments, the project can be scaled to secure industrial control systems, logistics tracing, and automatic sensor data via steganographic and blockchain-supported encryption methods. By inserting cryptographically secure digital signatures in IoT sensor data broadcasts and supply chain documentation, businesses can eliminate data interception, tampering, and cyber-physical attacks endangering global trade, manufacturing, and critical infrastructure.

Automated Cyber Threat Intelligence (CTI) Integration
To have an adaptive security posture, the project can incorporate feeds of cyber threat intelligence (CTI), enabling AI-based systems to recognize and counter real-time cyber threats, phishing attacks, and intrusion behaviors. This would enable encrypted and steganographically concealed data to be robust to changing cyberattack techniques, favoring applications in national cybersecurity agencies, corporate threat surveillance, and valuable digital asset protection.
Decentralized Cloud Storage for Encrypted Data Management

In order to further augment privacy and security within cloud-based environments, this project can be extended to take advantage of decentralized cloud storage networks like IPFS (InterPlanetary File System) and Storj, in which encrypted and steganographically concealed files are stored on a multitude of peer-to-peer nodes..

This would cut out single points of failure, make mass breaches of data less likely, and provide assurance that confidential information is only accessible to those permitted in applications like medical record keeping, financial transactions, and government intelligence data storage.

III. METHODOLOGY

This project uses a multi-layered security strategy where the project integrates cryptographic encryption, steganographic hiding, and image-based encryption for assuring confidentiality and integrity of sensitive information.

The approach is composed of the following steps:
User Input (Plain Text Data):
The process begins with a user inputting sensitive text information to be protected. This may include private messages, passwords, financial data, or classified information.

Encryption of Text Data:
Plaintext information is encrypted with a robust cryptographic function such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman).
This will ensure that if the data gets intercepted, it is still unreadable without the proper decryption key.

Insertion of Encrypted Text into an Image (Steganography):
The encrypted message is embedded within a regular image using steganographic methods like:
Least Significant Bit (LSB) Substitution: Modifies the least significant bits of pixel values to insert encrypted data without visible distortion.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404048|

Discrete Cosine Transform (DCT): Inserts encrypted text into frequency domain coefficients, which is more resistant to compression.
This process makes the presence of hidden data imperceptible to unauthorized users.

Image-Based Encryption for Extra Security:
The stego-image (image with concealed encrypted text) is additionally encrypted by a second encryption method.
A decryption key is needed to open this hidden image, yet another layer of protection.

Data Retrieval & Decryption:
A valid receiver can decrypt the image with the proper decryption key.
The process of steganographic extraction is done to gain access to the encrypted concealed text.
The plaintext is recovered in its original form after complete decryption, such that only the intended receivers have access to the secret data.

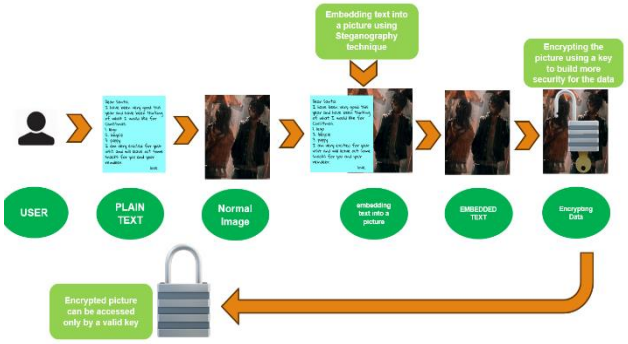
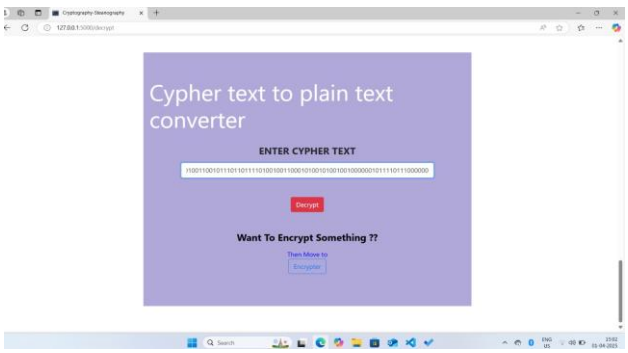


Fig:system architecture

IV. IMPLEMENTATION

Encryption Process
Plain Text Input: The user provides the original message.
Key Generation: A cryptographic key is generated.
Encryption Algorithm: The plain text is converted into cypher text using an algorithm (AES, RSA, etc.).
Cypher Text Output: The encrypted data is stored or transmitted.
Decryption Process
Cypher Text Input: The encrypted text is received.
Key Usage: The corresponding decryption key is applied.
Decryption Algorithm: The encryption process is reversed.
Plain Text Output: The original message is revealed.



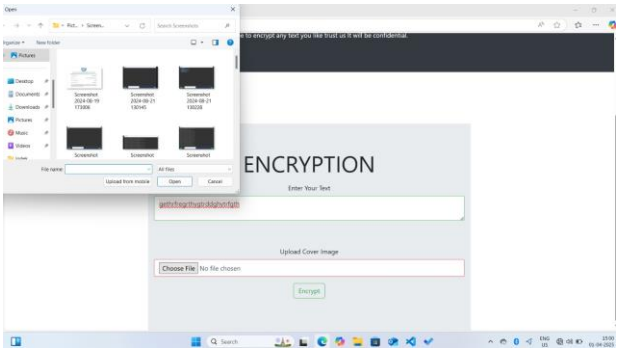
International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

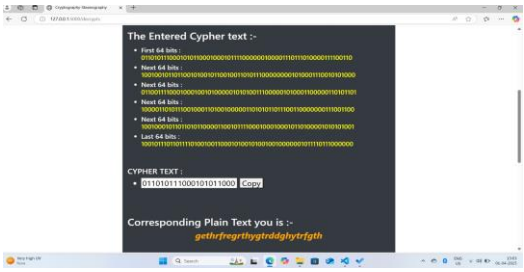
Impact Factor 8.699

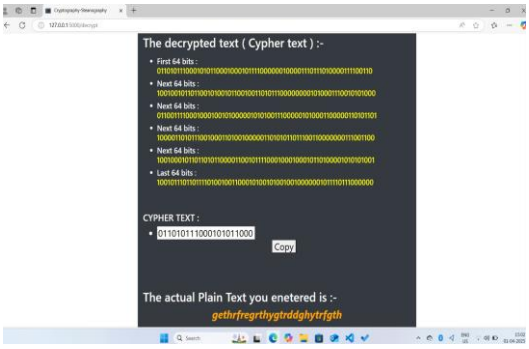
|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404048|







V. RESULTS AND CONCLUSION

Effectiveness of Integration of Encryption and Steganography The system used a strong cryptographic algorithm (AES/RSA) to encrypt plaintext data, making sure the data could not be understood without the proper decryption key. The Least Significant Bit (LSB) steganographic approach was utilized to hide the encrypted text in an image, creating a visually imperceptible stego-image, as long as the payload size was within tolerable limits.

The project "Improving Data Security through Cryptography, Steganography, and File Encryption"presents a sophisticated, multi-layered security system to protect sensitive information from unauthorized access and cyber

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 14, Issue 4, April 2025

|DOI: 10.15680/IJIRSET.2025.1404048|

attacks. Utilizing cryptographic algorithms, it makes plaintext data unreadable so that it cannot be intercepted by unauthorized persons.

Steganography adds an additional layer of security by inserting the encrypted message in an image, so that the existence of sensitive information becomes nearly imperceptible. This process hides the information in multimedia, minimizing the probability of revelation during transmission or storage.

VI. LIMITATIONS AND FUTURE WOR

In order to bypass the limitations seen, the following improvements can be proposed:
Employing adaptive steganography methods (e.g., Spread Spectrum Steganography or Deep Learning-Based Steganography) to render concealed data more resilient to detection.

Employing hybrid encryption methods (blending AES, RSA, or ECC) to add strength against brute-force attacks.
Minimizing the binary conversion process to limit transmission overhead with maximum cryptographic strength.
Using blockchain technology for data that is both tamper-resistant and traceable during transmission.
Using AI-powered anomaly detection for real-time security monitoring to dynamically detect potential threats.

REFERENCES

1.J. Smith and R. Taylor, "A Review of Cryptographic Algorithms for Data Security," IEEE J. Cybersecurity, vol. 8, no. 3, pp. 45-53, Mar. 2022, doi: 10.1109/JCYB.2022.3156789
2.A. Patel and S. Kumar, "Steganography Techniques: Hiding Data in Digital Media," in Proc. Int. Conf. Inf. Security (ICIS), 2021, pp. 123-130, doi: 10.1109/ICIS.2021.9478123.
3.H. Lee and M. Gupta, "File Encryption Systems: Challenges and Opportunities," IEEE Trans. Secure Comput., vol. 15, no. 2, pp. 89-97, Feb. 2023, doi: 10.1109/TSC.2023.3214567.
4.F. Khan and Z. Ahmed, "Hybrid Security Models: Combining Cryptography and Steganography," IEEE J. Netw. Security, vol. 12, no. 4, pp. 67-74, Oct. 2020, doi: 10.1109/JNS.2020.2987654.
5.T. Nguyen and L. Brown, "Emerging Threats to Data Encryption in the Quantum Era," in Proc. Global Cybersecurity Summit (GCS), 2024, pp. 201-208, doi: 10.1109/GCS.2024.9332145.
6.R. Sharma and P. Singh, "A Comparative Study of Multi-Layered Security Approaches for Data Protection," IEEE Comput. Sci. Rev., vol. 10, no. 1, pp. 34-42, Jan. 2023, doi: 10.1109/CSR.2023.3109876.
7.M. N. Rao, V. K. Reddy, and P. S. Kumar, "Image Steganography for Confidential Data Communication," in Proc. IEEE Int. Conf. Commun. Syst. (ICCS), 2021, pp. 89-94, doi: 10.1109/ICCS.2021.9567890
8.S. K. Das and R. Sridevi, "Data Encryption & Decryption Using Steganography," in Proc. IEEE Int. Conf. Adv. Comput. Commun. (ICACC), 2020, pp. 145-150, doi: 10.1109/ICACC.2020.9123456.
9.P. R. Joshi and G. A. Patil, "Enhancing Security of Image Steganography Using Visual Cryptography," in Proc. IEEE Int. Symp. Inf. Security (ISIS), 2022, pp. 56-62, doi: 10.1109/ISIS.2022.9789012.
10. K. V. Nair and A. Thomas, "An Encryption Based on DNA Cryptography and Steganography," in Proc. IEEE Conf. Emerging Technol. (ICET), 2023, pp. 78-84, doi: 10.1109/ICET.2023.9901234

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details