International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Steganography and Cryptography in Media Files

Divya Tyagi [1]
Dept of Information Science and Engineering (ISE) AMCEC
divyatyagi@amceducation.in

Kushal M [1], Chiranjeevi R K [2], Harsha R [3], Shubham Kumar [4]

Dept of information Science and Engineering (ISE)AMCEC
1am22is046@amceducation.in , 1am22is025@amceducation.in , 1am22is037@amceducation.in , 1am23is409@amceducation.in.

Abstract The rapid growth of digital communication has increased the demand for secure and tamper-proof information exchange. This project presents CryptoSteg Secure Suite, a hybrid security platform that integrates AES-based symmetric encryption with LSB image steganography to achieve confidential and covert message transmission. By combining cryptography with data-hiding techniques, the system delivers a robust multilayered security model capable of protecting sensitive data against modern cyber threats.

In this approach, sensitive messages are first encrypted using the Advanced Encryption Standard (AES), a fast and industry-accepted symmetric encryption algorithm that ensures strong confidentiality with efficient processing. The encrypted data is then embedded into digital images using the Least Significant Bit (LSB) steganography technique, which hides information within pixel values without causing noticeable visual distortion. This ensures that both the content and the existence of the message remain protected.

The system is implemented with a user-friendly Python Tkinter graphical interface, allowing users to easily perform encryption, embedding, extraction, and decryption operations. Additional features such as input validation, error handling, and image-quality preservation enhance reliability and usability. Experimental results demonstrate that the generated stego-images maintain high visual quality while securely carrying encrypted data.

By integrating AES encryption with LSB steganography, CryptoSteg Secure Suite demonstrates a practical and effective secure communication model. While AES protects the message content, steganography provides stealth by concealing the presence of data itself, for future enhancements, offering a scalable foundation for research in secure communication, digital forensics, and privacy-preserving technologies.

Key words: AES Encryption, Symmetric Cryptography, LSB Steganography , Secure Communication Python Tkinter.

1. INTRODUCTION

The digital communication and multimedia exchange has made data security a critical challenge in today's interconnected world. Sensitive information is frequently transmitted over public and unsecured networks, increasing the risk of interception, misuse, and unauthorized access. To address these concerns, advanced security techniques such as cryptography and steganography are widely used, as they play a vital role in protecting digital data and ensuring secure communication through media files.

Cryptography secures information by converting it into an unreadable encrypted form using mathematical algorithms and secret keys, allowing access only to authorized users. Symmetric encryption techniques are commonly employed due to their efficiency and strong confidentiality in protecting multimedia content. However, although cryptography ensures data privacy, the presence of encrypted data may still attract attention during transmission, making it vulnerable to detection or attack.

Steganography complements cryptography by concealing the existence of information within digital media such as images, audio, or video files. Techniques like Least Significant Bit (LSB) modification embed encrypted data into media files without noticeable degradation in quality. When

cryptography and steganography are combined, a powerful dual-layer security framework is achieved, ensuring both secrecy of content and invisibility of communication. This hybrid approach is widely applied in secure multimedia communication, digital rights management, and confidential data transmission.

2. Problem Statement

Digital media files are widely used for transmitting and storing confidential information, making them attractive targets for unauthorized access and data manipulation. While encryption techniques effectively protect the content of information, the presence of encrypted data can easily be identified, increasing the risk of interception. Steganographic methods attempt to overcome this limitation by embedding secret data within media files; however, these methods often face challenges related to limited hiding capacity, degradation of media quality, and vulnerability to detection through steganalysis or common media transformations.

To ensure secure and discreet communication, there is a need for a system that combines cryptographic protection with reliable steganographic embedding. The primary challenge is to design a hybrid approach that encrypts sensitive data and hides it within media files without affecting perceptual quality, while also ensuring resistance to unauthorized extraction and analysis. Such a system must provide both strong data confidentiality and effective concealment, making it suitable for secure media-based communication and data protection applications

3. Methodology

- Encryption Using AES (Symmetric Key)

The user's secret message is encrypted using the AES algorithm with a symmetric key to ensure confidentiality .The encrypted output is converted into binary form for steganographic embedding.

- Image Steganography Using LSB Technique

The encrypted binary data is embedded into the least significant bits of image pixels .This process preserves image quality while securely hiding the data.

- Audio and Video Steganography

Encrypted data is embedded into audio using transform-domain techniques to improve robustness .In video steganography, data is distributed across frames to increase security and capacity.

- Extraction and Decryption Process

The embedded encrypted data is extracted from the stego media using the same technique.AES decryption with the correct key restores the original message.

- User Interface and System Integration

A Tkinter-based interface allows users to perform encryption and steganographic operations easily. Real-time feedback and error handling ensure smooth and secure system usage.

4. Implementation

The implementation of the proposed system is carried out using Python, integrating cryptography and steganography techniques to secure data within media files. Initially, the user's secret message is encrypted using the Advanced Encryption Standard (AES), a symmetric-key algorithm that provides strong confidentiality and fast execution. A secret key is generated or supplied by the user, and the resulting ciphertext is converted into binary form to prepare it for embedding into digital media.

The encrypted binary data is embedded into media files using appropriate steganographic techniques. For image files, the Least Significant Bit (LSB) method is applied to hide data within pixel values while preserving visual quality. For audio and video files, transform-domain techniques are used to embed data into selected coefficients or frames, improving robustness against noise, compression, and common processing operations. These methods ensure that the hidden data remains imperceptible and does not degrade the quality of the original media.

The extraction and recovery process follows the reverse workflow, where the stego media file is selected and the embedded encrypted data is retrieved using the same steganographic technique. The extracted data is then decrypted using the same AES symmetric key to recover the original message. A Python Tkinter-based graphical interface facilitates all operations, providing user-friendly interaction, validation, and error handling.

5. Result and Discussion

The implementation and testing of the proposed steganography and cryptography system demonstrate that the integration of AES encryption with media-based steganography provides effective and reliable data security. The experimental results confirm that AES successfully encrypts sensitive messages, ensuring confidentiality before embedding. The encrypted data was embedded into image, audio, and video files using appropriate steganographic techniques without causing noticeable degradation in media quality. Image steganography using the LSB method preserved visual clarity, while audio and video steganography maintained perceptual quality and robustness against common processing operations.

During the extraction process, the system accurately retrieved the embedded encrypted data from the stego media files. When the correct symmetric key was provided, the original message was recovered without any loss, whereas the use of an incorrect key resulted in unreadable output, validating the effectiveness of the encryption mechanism. These results highlight the advantage of the dual-layer security approach, where cryptography protects the content of the data and steganography conceals its existence. Overall, the system achieves a good balance between security, imperceptibility, and data capacity, making it suitable for secure communication through media files and providing a strong foundation for future enhancements.

6. Conculsion

This project successfully demonstrates a secure and efficient approach for protecting sensitive information by integrating cryptography with steganography in digital media files. By encrypting secret messages using the Advanced Encryption Standard (AES) and embedding the encrypted data within images, audio, and video files, the system ensures both confidentiality and concealment of information. The use of media-based steganographic techniques preserves the quality of the original files while securely hiding the encrypted content.

The experimental results confirm that the proposed system effectively resists unauthorized access and detection. Even if the hidden data is discovered, it remains unreadable without the correct symmetric key, providing a strong dual-layer security mechanism. The system also maintains a balance between data capacity, imperceptibility, and robustness against common media processing operations.

Overall, the proposed solution offers a practical, user-friendly, and reliable method for secure communication through media files. With its modular design and Python-based implementation, the system provides a strong foundation for future enhancements such as improved robustness, increased payload capacity, and support for additional media formats, making it suitable for real-world secure communication applications.

6. REFERENCES

[1] Tripathi, R., Umrao, L. S., and Tripathi, A. (2024). Review on Metamorphic Cryptography: A Combined Approach of Cryptography & Steganography Techniques. Proceedings of the First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT) ,IEEE,pp.237–242.IEEEXplore, link

[2] Supriya, S. K., and Lovesum, J. S. P. (2024). Review on Lightweight Cryptography Techniques and Steganography Techniques for IoT Environment. International Journal of System Assurance Engineer- - ing and Management, 15, 4210–4228. Springer, link

[3] Solomon Raj, U. A., and Maheswaran, C. P. (2023). Secure File Sharing System Using Image Steg- -anography and Cryptography Techniques. Proceedings of the International Conference on Inventive C omputation Technologies (ICICT), IEEE, pp. 1113–1118. IEEE Xplore, link

[4] Srinivasan, D., Manojkumar, K., Syed, A., and Nutakki, H. (2024). A Comprehensive Review on A- - dancements and Applications of Steganography. Preprint, March 2024. ResearchGate, link