IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, March 2026
Impact Factor: 8.2

Crypto Lens: An Advanced Steganography Suite for Secure Data Hiding and Detection

Miss. Manasi Dnyaneshwar Patil[1], Miss. Tirtha Sachin Mogarkar[2], Mr. Samiksha Anil Patil[3], Mrs. Shilpa Makarand Jadhav[4]
Students, Department of Computer Technology[1,2,3]
Guide, Department of Computer Technology[4]
Bharati Vidyapeeth Institute of Technology Kharghar, Navi Mumbai, Maharashtra, India

Abstract: *In the modern digital era, secure communication is essential due to increasing cyber threats and data breaches. This paper presents Crypto Lens: An Advanced Steganography Suite for Secure Data Hiding and Detection, a dual-layer security framework that integrates cryptography and steganography within a unified system.*

The proposed approach encrypts secret data using the Advanced Encryption Standard (AES) with password-based key derivation and ensures data integrity through HMAC with SHA-256. The encrypted content is embedded into image and audio files using the Least Significant Bit (LSB) steganography technique to achieve covert communication with minimal perceptual distortion.

The system supports multiple file formats and is implemented using Python with a graphical user interface built on PySide6 and QML.Experimental results demonstrate that the framework effectively achieves confidentiality, integrity, and hidden data transmission while preserving media quality.

Keywords: Cryptography, Steganography, AES Encryption, HMAC, LSB Technique, Secure Communication, Data Integrity

I. INTRODUCTION

The rapid growth of digital communication technologies has significantly increased the exchange of sensitive information across networks. With this expansion, cyber threats, data breaches, and unauthorized access have become major concerns in modern computing environments. Ensuring confidentiality, authenticity, and secure transmission of data has therefore become a critical requirement for individuals and organizations. Cryptography plays a fundamental role in protecting digital information by converting plaintext into unreadable ciphertext using mathematical algorithms. One of the most widely accepted encryption standards is the Advanced Encryption Standard (AES), known for its strong security and computational efficiency.

Although encryption ensures data confidentiality, it does not hide the presence of communication. Encrypted files may attract attention and become potential targets for interception or cryptanalysis. To overcome this limitation, steganography is employed to conceal secret information within digital media such as images and audio files.

The Least Significant Bit (LSB) technique is commonly used due to its simplicity and minimal impact on media quality. By embedding information into the least significant bits of pixels or audio samples, hidden data remains imperceptible to human observation.

However, many existing systems focus either on encryption or steganography independently and often lack mechanisms for integrity verification. To address these limitations, the proposed system, Crypto Lens, integrates encryption, steganography, and authentication within a unified framework. The system encrypts secret data using AES, verifies integrity using Hash-based Message Authentication Code (HMAC) with SHA-256, and embeds encrypted data into carrier media using LSB-based techniques. The primary contribution of this work is the development of a dual-layer security framework that ensures confidentiality, concealment, and tamper detection within a single user-friendly platform.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, March 2026
Impact Factor: 8.2

II. MOTIVATION

In the current digital ecosystem, sensitive information is frequently transmitted through online platforms, cloud services, and multimedia communication channels. Despite the availability of advanced encryption techniques, cyber threats such as interception, unauthorized access, and data manipulation continue to increase. While encryption protects the content of data, it does not prevent attackers from identifying the presence of secured communication. Encrypted files may raise suspicion and become potential targets for cryptanalysis.

Steganography offers a complementary approach by concealing the existence of communication within digital media. However, many existing steganographic systems lack strong encryption mechanisms and fail to provide integrity verification. Hidden data may be vulnerable to tampering, modification, or corruption without detection. Furthermore, most available tools focus on a single media type and do not provide an integrated, user-friendly platform that combines confidentiality, concealment, and authentication.

The motivation behind Crypto Lens is to develop a unified framework that integrates cryptographic security, covert data hiding, and integrity verification within a single system. By combining AES encryption, HMAC-based authentication, and LSB steganography for both image and audio media, the proposed system aims to provide enhanced security, reliability, and practical usability for secure digital communication.

III. LITERATURE SURVEY

Secure communication has been an active area of research in the field of information security. Both cryptography and steganography have evolved significantly to address confidentiality and protection challenges in digital systems. Johnson et al. [3] and Kumar & Pooja [6] discussed various data hiding and security mechanisms for protecting digital information.

The Advanced Encryption Standard (AES), proposed by Daemen and Rijmen [8], is one of the most widely adopted symmetric encryption algorithms. It is standardized by NIST and is known for its strong resistance against brute-force and cryptanalytic attacks. Stallings [7] emphasized that AES provides high security with efficient performance, making it suitable for modern secure communication systems.

Steganography techniques, particularly image-based methods, have been extensively studied. Saleh [1] provided a detailed review of various image steganography techniques. Singh et al. [2] demonstrated that the Least Significant Bit (LSB) technique is a simple yet effective spatial-domain approach that introduces minimal perceptual distortion. Morkel et al. [4] further analyzed the applications of image steganography in secure communication systems, while Reddy et al. [5] implemented LSB techniques for multiple file formats.

Audio steganography has also gained importance due to redundancy in audio signals. Kumar and Pooja [6] and Khan [10] highlighted that LSB substitution in audio samples enables covert data transmission with negligible impact on sound quality.

While steganography conceals the presence of communication, it does not guarantee confidentiality. Johnson et al. [3] suggested combining encryption with steganography for enhanced security. The integration of AES encryption with steganographic techniques has been explored to provide dual-layer protection [7][8].

Data integrity verification is another critical requirement in secure systems. Krawczyk et al. [9] introduced the HMAC mechanism, which uses cryptographic hash functions such as SHA-256 to ensure message authenticity and detect tampering.

Despite these advancements, many existing systems focus either on encryption or steganography individually and lack integrated integrity verification. Additionally, limited solutions support multiple media formats within a unified interface. The proposed system, Crypto Lens, addresses these gaps by integrating AES encryption, HMAC-based authentication, and LSB-based image and audio steganography within a single practical framework.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, March 2026
Impact Factor: 8.2

IV. PROPOSED SYSTEM

The proposed system, Crypto Lens: An Advanced Steganography Suite for Secure Data Hiding and Detection, is designed to provide a dual-layer security framework by integrating cryptography and steganography within a unified platform. The system ensures confidentiality, concealment, and integrity verification of sensitive digital data.

The core objective of the system is to protect secret information by first encrypting it and then embedding it into digital media files such as images and audio. This approach ensures that even if the hidden data is discovered, it remains unreadable without proper authentication.

The system operates in two major phases: Data Hiding (Sender Side) and Data Extraction & Verification (Receiver Side).

In the Data Hiding phase, the user selects a carrier media file, which can be an image (such as .png or .jpg) or an audio file (such as .wav). The user then selects or enters the secret data, which may include text files, PDF documents, or image files. The secret data is encrypted using the Advanced Encryption Standard (AES) with password-based key derivation to ensure confidentiality.

After encryption, a Hash-based Message Authentication Code (HMAC) using SHA-256 is generated for the encrypted data. This HMAC value is appended to the encrypted content to enable integrity verification and tamper detection during extraction.

The encrypted data along with the generated HMAC is then embedded into the selected carrier media using the Least Significant Bit (LSB) steganography technique. In the case of images, the least significant bits of pixel values are modified, while for audio files, the least significant bits of audio samples are altered. These modifications are minimal and do not cause perceptible distortion to the carrier media.

In the Data Extraction phase, the receiver uploads the stego media file into the system. The hidden bits are extracted using the LSB extraction algorithm, and the encrypted data is separated from the HMAC value. The system recalculates the HMAC and compares it with the extracted value. If the values match, data integrity is confirmed. If they do not match, tampering is detected.

Upon successful verification, the encrypted data is decrypted using the correct password, and the original secret file is restored.

The system is implemented using Python with a graphical user interface developed using PySide6 and QML. The modular design ensures systematic execution of encryption, embedding, extraction, and verification processes within a single user-friendly platform.

V. PROPOSED FRAMEWORK

The proposed framework of Crypto Lens is structured as a sequential and modular security model that integrates encryption, authentication, and steganographic embedding within a unified workflow. The framework ensures confidentiality, integrity, and covert communication through a dual-layer security mechanism.

The overall architecture of the system consists of two primary modules: the Sender Module and the Receiver Module.

A. Sender Module

The sender module performs secure data preparation and embedding. The process begins with the selection of a carrier media file, which may be an image or an audio file. The selected media serves as the host file for hiding confidential information.

After media selection, the user provides the secret data that needs to be protected. The system supports multiple file formats including text, PDF, and image files. The secret data is then processed through an encryption module where it is encrypted using the Advanced Encryption Standard (AES) with password-based key derivation. This ensures that the original content is converted into secure ciphertext.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, March 2026
Impact Factor: 8.2

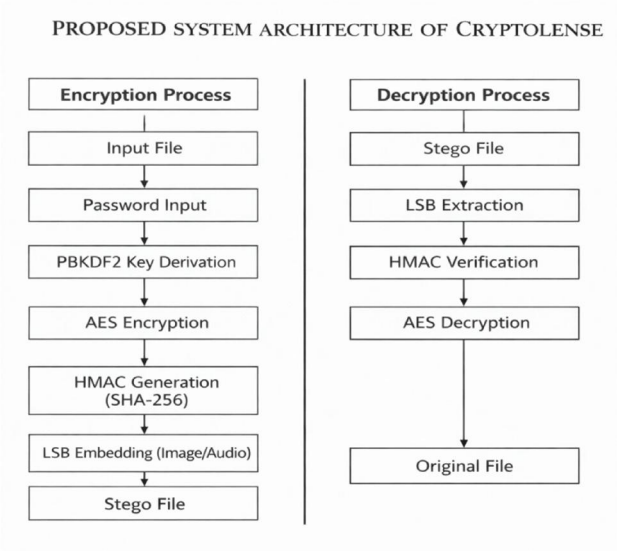

Fig.1 Workflow Diagram Of Crypto Lense

Following encryption, a Hash-based Message Authentication Code (HMAC) using SHA-256 is generated for the encrypted data. This authentication code is appended to the ciphertext to enable verification of integrity during extraction.

The encrypted data along with the generated HMAC is passed to the steganography module. The system applies the Least Significant Bit (LSB) embedding technique to hide the encrypted content within the carrier media. In images, pixel-level least significant bits are modified, while in audio files, least significant bits of audio samples are altered. The output of this stage is the stego file, which appears visually or audibly unchanged but contains hidden encrypted information.

B. Receiver Module

The receiver module is responsible for data extraction, verification, and recovery. The receiver uploads the stego media file into the system. The LSB extraction algorithm retrieves the hidden bit stream from the carrier file.

The extracted data is separated into two components: encrypted data and the corresponding HMAC value. The system recalculates the HMAC using the extracted encrypted data and compares it with the received authentication code. If both values match, the integrity of the data is verified. If a mismatch occurs, the system detects tampering and prevents decryption.

Upon successful verification, the encrypted data is decrypted using the correct password through the AES decryption module. The original secret file is then reconstructed and restored to its initial format.

Framework Characteristics

The proposed framework provides the following key features:

- Confidentiality through AES encryption.
- Integrity verification using HMAC with SHA-256.
- Covert communication via LSB-based image and audio steganography.
- Multi-format support for secret data embedding.
- User-friendly operation through a graphical interface developed using PySide6 and QML.
- The structured and layered design of the framework ensures secure, reliable, and tamper-resistant digital communication.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 6, March 2026
Impact Factor: 8.2

VI. CONCLUSION

The proposed system, Crypto Lens: An Advanced Steganography Suite for Secure Data Hiding and Detection, presents a structured and integrated approach for secure digital communication. The system successfully combines encryption, steganography, and authentication within a unified framework to ensure confidentiality, concealment, and data integrity.

The use of Advanced Encryption Standard (AES) provides strong protection against unauthorized access, while the implementation of Hash-based Message Authentication Code (HMAC) using SHA-256 ensures tamper detection and message authenticity. The Least Significant Bit (LSB) technique enables covert embedding of encrypted data into image and audio files with minimal perceptual distortion.

The modular architecture and graphical interface developed using Python and PySide6 enhance usability and operational efficiency. The framework supports multiple file formats and demonstrates reliable performance during encryption, embedding, extraction, and verification processes.

By integrating dual-layer security mechanisms within a single platform, Crypto Lens offers a practical and effective solution for covert and secure digital communication. The proposed framework addresses the limitations of systems that rely solely on encryption or steganography and establishes a foundation for further advancements in secure multimedia communication systems.

REFERENCES

[1]. Mohammed A. Saleh, Image Steganography Techniques, IJARCCE, 2018.
[2]. Mohammed A. Saleh, “Image Steganography Techniques: A Review,” IJARCCE, vol. 7, no. 4, pp. 45–49, 2018.
[3]. Arun K. Singh, S. K. Singh, “Steganography in Images Using LSB Technique,” IJLTET, vol. 5, no. 2, pp. 15–20, 2015..
[4]. T. Morkel, J. H. P. Eloff, M. S. Olivier, “An Overview of Image Steganography,” University of Pretoria, 2012.
[5]. V. L. Reddy, A. Subramanyam, “Implementation of LSB Steganography for Various File Formats,” IJANA, vol. 3, no. 5, 2011.
[6]. Arvind Kumar, Km. Pooja, “Steganography – A Data Hiding Technique,” International Journal of Computer Applications, vol. 9, no. 7, 2010.
[7]. W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson, 2017.
[8]. J. Daemen, V. Rijmen, “AES Proposal: Rijndael,” NIST AES Submission, 1999.
[9]. H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-Hashing for Message Authentication,” RFC 2104, 1997.
[10]. M. K. Khan, “A Survey of Steganography Techniques in Image, Audio, and Video,” Information Technology Journal, vol. 12, no. 2, 2013.