Stegovaultpro: Secure Multi-Format Steganography for Confidential Data Hiding

Sarjun Chanakya S.K and Dr. B. Leelavathi

1.Student, Department of Computer Technology, Dr.N. G. P. Arts and Science College, Coimbatore, India, E-Mail: 231CT145@drngpasc.ac.in

2.Professor, Department of Computer Technology, Dr.N. G. P. Arts and Science College, Coimbatore, India,

E-Mail: get2leelavathi@gmail.com

https://doi.org/10.55041/ijsmt.v2i3.088

Cite this Article: S.K, S. C. (2026). Stegovaultpro: Secure Multi-Format Steganography for Confidential Data Hiding. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.088

ABSTRACT

Steganography is a technique used to hide confidential information within digital media files in such a way that the existence of the hidden data remains unnoticed. This project presents StegoVaultPro, a secure multi-format steganography platform designed to embed and extract hidden messages across multiple carrier types including images, audio, video, and text files. The system integrates Least Significant Bit (LSB) embedding techniques with strong cryptographic protection using AES encryption in Cipher Block Chaining (CBC) mode combined with PBKDF2 key derivation to ensure message confidentiality before embedding.

The platform is implemented as a modular web-based application that provides a centralized dashboard for performing encoding and decoding operations. It supports carrier formats such as PNG, JPG, WAV, MP4, TXT, and PDF, allowing flexible multimedia steganography operations. Additional security mechanisms including password protection, input validation, and controlled decryption handling ensure safe processing of user data. Experimental observations demonstrate efficient embedding performance, reliable message recovery, and minimal perceptual distortion of carrier files. The proposed system offers a scalable and extensible framework for secure multimedia information hiding.

KEYWORDS

Steganography,Information Hiding, AES Encryption, PBKDF2, Least Significant Bit, Multimedia Security, Data Protection.

1. INTRODUCTION

With the rapid expansion of digital communication technologies, the need for secure transmission of confidential information has become increasingly important. Traditional security approaches such as encryption protect the content of information but do not conceal the presence of the communication itself. Encrypted data can still attract attention and may become a target for attackers. Steganography provides an alternative solution by hiding secret information inside ordinary digital media files so that the communication appears normal and does not raise suspicion.

Modern communication systems use various types of multimedia data including images, audio, video, and text documents. However, many existing steganography systems focus only on hiding data within a single type of media file. These systems often lack integrated encryption mechanisms and structured user interfaces, which limits their practical usability and security level.

The proposed system StegoVaultPro addresses these limitations by providing a unified platform for secure multimedia steganography. The system allows users to embed encrypted messages within different carrier files while maintaining the visual or auditory quality of the original media. By combining cryptographic protection with steganographic embedding techniques, the platform enhances confidentiality and reduces the risk of unauthorized data extraction.

2. PROBLEM STATEMENT

Existing steganography tools often provide limited functionality and support only a single carrier format such as images. Most traditional implementations rely solely on Least Significant Bit embedding techniques without applying strong encryption mechanisms. As a result, if hidden information is detected through steganalysis, the extracted message may be directly readable.

Another limitation of many existing systems is the absence of a centralized interface for managing steganographic operations. Users must rely on separate tools for different media types, which increases complexity and reduces efficiency. Additionally, traditional systems frequently lack proper input validation and secure key derivation mechanisms, which may expose sensitive information to security risks.

Therefore, there is a requirement for a secure, flexible, and user-friendly steganography platform that supports

multiple carrier formats while providing integrated encryption, structured workflow management, and reliable data protection.

3. LITERATURE REVIEW

Information security is an important aspect of modern digital communication systems due to increasing risks of data interception and unauthorized access. Steganography and cryptography are widely used techniques for protecting confidential information by hiding or encrypting data during transmission. Several researchers have explored different approaches to improve the security and efficiency of information hiding systems.

Johnson, Duric, and Jajodia [1] explained the fundamental concepts of information hiding and described how steganography can conceal secret data within digital media such as images, audio, and video files. Katzenbeisser and Petitcolas [2] discussed various techniques used for embedding hidden information in multimedia carriers and emphasized the importance of maintaining carrier quality during the embedding process.

Stallings [3] highlighted the role of cryptography in protecting sensitive information in communication systems. Encryption algorithms such as AES provide strong protection by converting plain data into unreadable formats. Schneier [4] further discussed the design and implementation of cryptographic algorithms and their importance in building secure digital systems.

Anderson [5] examined security engineering principles and explained how secure system architectures can protect sensitive data and ensure reliable communication. Menezes, van Oorschot, and Vanstone [6] presented comprehensive research on applied cryptography and key management techniques used to strengthen data protection in secure communication environments.

Wayner [7] introduced the concept of disappearing cryptography, where encrypted information is hidden within digital media using steganographic techniques. Provos and Honeyman [8] studied practical steganography implementations and demonstrated how hidden data can be embedded within images without noticeable changes to the carrier file.

Petitcolas [9] explored various applications of information hiding and explained how steganography can be applied in multimedia security and secure communication systems. Leelavathi and Rajesh M. Babu [10] proposed an efficient detection system using multi-featureanalysis to identify malicious worms in networks, demonstrating how advanced analysis techniques can detect hidden patterns in data.

Overall, previous research shows that combining cryptography with steganography can significantly improve the security of digital communication systems by protecting both the content and the existence of confidential information.

4. PROPOSED SYSTEM

The proposed system StegoVaultPro is designed to provide a secure and modular platform for performing steganographic operations across multiple types of digital media. The system enables users to embed confidential information inside carrier files such as images, audio, video, and text documents while maintaining the original appearance or quality of the media.

Before embedding the secret message into the carrier file, the system provides an optional encryption step using AES-CBC encryption. The encryption key is generated through the PBKDF2 key derivation function based on the user-provided password. This additional security layer ensures that even if hidden data is extracted from the carrier media, it cannot be interpreted without the correct password.

The platform includes a centralized dashboard that allows users to access different steganography modules. Each module provides both encoding and decoding operations and supports secure handling of multimedia carrier files.

4.1 Architecture of the System

The system architecture follows a modular layered design consisting of a user interface layer, processing layer, encryption module, and steganographic embedding engine. Users interact with the application through the dashboard interface where they can select the desired steganography module and upload carrier files. The backend processes the user input by performing encryption, binary conversion, and data embedding operations. The modular architecture ensures clear separation between user interaction, cryptographic operations, and steganographic algorithms, which improves system scalability and maintainability.

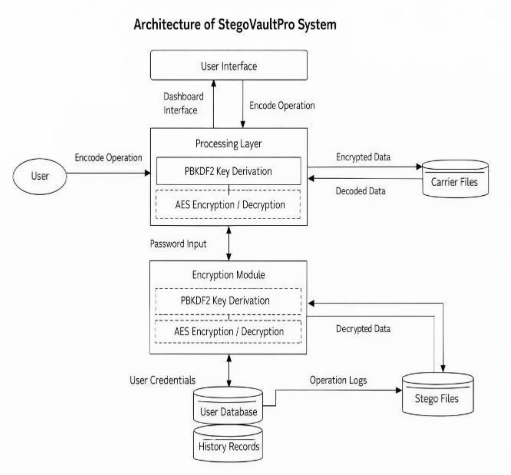

FIGURE 1: ARCHITECTURE OF THE SYSTEM

4.2 Core Mechanism / Module 1

The first core mechanism focuses on encryption and key derivation. When the user chooses password protection, the secret message is encrypted before embedding. The password is processed using PBKDF2 to derive a secure cryptographic key, which is then used in AES-CBC encryption.

This mechanism ensures that the hidden message remains confidential even if the embedded data is detected and extracted from the carrier media.

4.3 Core Mechanism / Module 2

The second module implements the steganographic embedding process. For image and audio carriers, the system uses Least Significant Bit modification techniques to embed binary data into pixel values or audio samples. For video carriers, selected frames are modified to store hidden information without affecting playback quality.
In text carriers such as TXT and PDF files, hidden Unicode characters or encoding- based techniques are used to insert concealed information without altering visible content.

4.4 Core Mechanism / Module 3

The third module manages the data extraction and decoding process. During decoding, the system scans the stego file and retrieves the hidden binary data embedded within the carrier media. If encryption was applied during embedding, the extracted data is decrypted using the password provided by the user.

This process ensures accurate recovery of the original secret message while maintaining security controls.

4.5 Performance Evaluation Metrics

The performance of the proposed system is evaluated using everal parameters including embedding efficiency, processing time, and carrier quality preservation. These metrics help determine the effectiveness of the steganographic algorithms and the overall system performance**.**

4.6 Advantages of the Proposed System

The proposed platform offers improved security by combining encryption with steganographic techniques. It supports multiple carrier formats and provides a centralized dashboard for managing operations. The modular design allows easy extension of the system with additional algorithms and advanced security features.

5. METHODOLOGY

The methodology describes the structured approach used to design and implement the steganography platform. The system processes user input through a sequence of stages including encryption, embedding, extraction, and decryption. Each stage is carefully designed to ensure security, reliability, and efficiency in handling multimedia data.

5.1 System Modeling

The system is modeled as a data processing workflow consisting of input acquisition, encryption, embedding, extraction, and output generation stages. Each stage interacts with the others through defined data flows that maintain structured processing.

5.2 Task Scheduling / Data Processing Mechanism

The application processes encoding and decoding requests sequentially through the selected steganography module. When a user uploads a carrier file and enters a secret message, the system converts the message into binary form and embeds it within the carrier media.

5.3 Failure Injection / Simulation Model

Failure conditions are simulated by providing invalid input formats, corrupted files, or incorrect passwords. These scenarios help evaluate the system's robustness and ensure that appropriate error handling mechanisms are implemented.

5.4 Recovery & Adaptive Mechanism

The system includes error handling and validation mechanisms that prevent unauthorized decoding attempts. If an incorrect password is provided during decryption, the system stops the process without exposing any partial information**.**

5.5 Performance Evaluation Metrics

Performance evaluation focuses on measuring embedding efficiency, system response time, and the accuracy of message extraction across different carrier formats.

5.6 Metric 1 Explanation

Embedding efficiency refers to the ability of the system to hide secret datawithin a carrier file while maintaining minimal increase in file size.

5.7 Metric 2 Explanation

Processing time measures the duration required for encoding and decoding operations across different media formats.

5.8 Metric 3 Explanation

Carrier integrity evaluates the degree to which the original visual or auditory quality of the carrier file is preserved after embedding.

6. SYSTEM FLOW

The system flow begins when the user logs into the StegoVaultPro platform and selects a steganography module such as image, audio, video, or text. The user uploads a carrier file and enters the secret message to be hidden. If encryption is enabled, the message is first encrypted using AES before embedding.

The embedding engine then hides the encrypted message within the carrier media using the Least Significant Bit (LSB) technique and generates a stego file, which can be downloaded by the user. During decoding, the user uploads the stego file, and the system extracts the hidden data and decrypts it if encryption was applied, finally displaying the recovered secret message.

7. IMPLEMENTATION

7.1. User Authentication Module

The User Authentication Module manages user login and access control within the system. It allows users to securely sign in using a username and password before accessing the steganography dashboard. The module verifies user credentials and prevents unauthorized access to the system. After successful authentication, the user is redirected to the main dashboard where different steganography modules can be accessed. This module ensures basic security and user session management.

7.2 Dashboard and Navigation Module

The Dashboard Module acts as the central interface of the application. It provides users with access to different steganography functionalities such as image, audio, video, and text steganography. The dashboard also displays system status information and operational guidance for secure data hiding. Users can navigate easily between modules using the sidebar menu. This module improves usability by organizing all system functions in a structured interface.

7.3. Image Steganography Module

The Image Steganography Module enables users to hide secret messages within image files such as PNG and JPG. The system uses the Least Significant Bit (LSB) technique to embed binary data into the pixel values of the image without causing visible distortion. During the encoding process, the secret message is converted into binary form and inserted into the least significant bits of image pixels. During decoding, the system extracts the embedded bits and reconstructs the hidden message.

7.4 Audio Steganography Module

The Audio Steganography Module allows users to embed secret messages within audio carrier files such as WAV files. Similar to image steganography, the module modifies the least significant bits of audio samples to hide the message. The embedding process preserves the original sound quality so that the modifications remain imperceptible to human hearing. During decoding, the system reads the modified audio samples and retrieves the hidden binary data to reconstruct the original message.

7.5 Video Steganography Module

The Video Steganography Module hides confidential messages within video files such as MP4. The module processes video frames and embeds secret data into selected frames using LSB modification techniques. By modifying only specific frames and pixel values, the system ensures that the visual quality and playback of the video remain unaffected. During extraction, the system scans the embedded frames and retrieves the hidden information from the stego video file.

7.6 Text Steganography Module

The Text Steganography Module hides information within text-based carrier files such as TXT or PDF. Instead of modifying visible text, the system uses hidden Unicode characters and encoding patterns to insert secret data. These invisible characters allow information to be concealed within the text structure without altering its appearance. During decoding, the system detects these hidden characters and reconstructs the original message.

7.7 Encryption Module

The Encryption Module provides additional security by encrypting the secret message before embedding. The system uses the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode to protect the message content. A secure cryptographic key is generated using the PBKDF2 key derivation algorithm based on the password provided by the user. This module ensures that even if the hidden data is extracted, it cannot be interpreted without the correct password.

7.8 History and Logging Module

The History Module records metadata about steganographic operations performed by the user. It stores details such as operation type (encode or decode), carrier type, file name, encryption status, and timestamp. This information allows users to review previous operations and track system activity. The module improves transparency and helps maintain a record of system usage.

8. RESULT

8.1 Initial System Setup

The system was deployed as a web- based platform supporting multiple steganography modules for images, audio, video, and text.

8.2 Failure Scenario

Incorrect password input during decoding demonstrates the security mechanism preventing unauthorized message recovery.

8.3 Recovery Outcome

When the correct password is provided, the system successfully extracts and decrypts the hidden message from the stego file.

8.4 Performance Metrics Table

Experimental observations show efficient embedding operations with minimal distortion of the carrier media.

8.5 Analysis of Key Metric

Embedding efficiency and carrier quality preservation confirm that the system effectively hides data while maintaining media integrity.

8.6 Interpretation of Results

The results demonstrate that StegoVaultPro provides a secure and reliable solution for multimedia steganography with integrated encryption protection.

9. CONCLUSION

StegoVaultPro provides a secure and flexible platform for hiding confidential information within multimedia files. By combining AES encryption with steganographic techniques, the system enhances data protection while preserving carrier integrity. The modular architecture and user-friendly interface make the platform suitable for secure digital communication environments. The system can be further extended with advanced steganographic algorithms and steganalysis detection capabilities.

10. REFERENCES

[1] N. F. Johnson, Z. Duric, and S. Jajodia, Information Hiding: Steganography and Watermarking. Boston, MA, USA: Kluwer Academic Publishers, 2001.

[2] S. Katzenbeisser and F. A. P. Petitcolas, Information Hiding Techniques for Steganography and Digital Watermarking. Boston, MA, USA: Artech House, 2000.

[3] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Boston, MA, USA: Pearson Education, 2017.

[4] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY, USA: John Wiley & Sons, 1996.

[5] R. Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd ed. Indianapolis, IN, USA:Wiley Publishing, 2008.

[6] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. Boca Raton, FL, USA: CRC Press, 1996.

[7] P. Wayner, Disappearing Cryptography: Information Hiding—Steganography and Watermarking, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann, 2002.

[8] N. Provos and P. Honeyman, “Hide and Seek: An Introduction to Steganography,”IEEE Security & Privacy Magazine, vol. 1, no. 3, pp. 32–44, 2003.

[9] F. A. P. Petitcolas, Information Hiding: Techniques and Applications. Norwood, MA, USA: Artech House, 1999.

[10] Dr. Leelavathi and Rajesh M. Babu,“An Efficient Worm Detection System Using Multi Feature Analysis and Classification Techniques,” International Conference on Computer Networks, Springer Nature Link, pp. 1054–1064, 2019.