

SECURE CHAIN HIDE: BLOCKCHAIN-ENABLED AI STEGANOGRAPHY FOR MULTI-MODEL DATA

Vignesh.K¹, Ameeroddin.SK², Tushith.N³, Sathvik kumar.S⁴

¹²³⁴Department of Information Technology, TKR College of Engineering and Technology, Telangana, India

Abstract - The rapid growth of digital communication has increased the need for secure methods to protect sensitive multimedia information from unauthorized access. This project presents a secure multimedia data hiding approach that combines image steganography with Advanced Encryption Standard (AES) encryption to ensure both confidentiality and invisibility of the transmitted data. In the proposed system, secret multimedia content such as text, audio, or images is first encrypted using AES to provide strong cryptographic security. The encrypted data is then embedded into a cover image using image steganography techniques, making the presence of hidden information imperceptible to human vision. This dual-layer security model protects data even if the stego-image is intercepted, as the embedded content remains encrypted and unreadable without the correct key. Experimental results demonstrate that the method maintains high image quality, minimal distortion, and robust resistance against common steganalysis attacks. The proposed approach is suitable for secure communication in applications such as confidential data transmission, digital watermarking, and multimedia security systems.

Key Words: Image steganography, Advanced Encryption Standard (AES), multimedia security, data hiding, secure communication, cryptography, steganalysis resistance, information security.

1. INTRODUCTION

In today's digital era, the secure transmission of sensitive information over open networks has become a critical challenge. With the rapid growth of internet-based communication, data such as personal messages, confidential documents, medical records, and multimedia files are increasingly vulnerable to unauthorized access, interception, and cyberattacks. Traditional security techniques like cryptography protect data by converting it into unreadable formats, but they often reveal the existence of secret communication, making them attractive targets for attackers. Steganography offers an additional layer of security by concealing the very existence of secret data within digital media such as images, audio, or video files. Image steganography, particularly Least Significant Bit (LSB) encoding, is widely used due to its simplicity, efficiency, and minimal impact on image quality. However, steganography alone does not guarantee complete security if the hidden data is discovered. To overcome this limitation, the proposed system integrates AES (Advanced Encryption Standard) encryption with image steganography to ensure both data

confidentiality and invisibility. Before embedding, the secret data is encrypted using AES, making it unreadable even if extracted by an unauthorized user. The encrypted data is then hidden inside a cover image using LSB steganography, resulting in a stego image that appears visually identical to the original image. This project, Secure Multimedia Data Hiding Using Image Steganography and AES Encryption, provides a robust and secure framework for hiding and transmitting multimedia data over digital channels. By combining cryptographic security with steganographic techniques and implementing the system using the Django framework, the solution ensures secure user authentication, controlled access, and reliable data embedding and extraction, making it suitable for real-world applications such as secure communication, digital watermarking, and confidential data exchange.

1.1 Image Steganography for Secure Data Hiding

Image steganography is a technique used to conceal secret information within a digital image in such a way that the existence of the hidden data is not noticeable to human observers. Unlike cryptography, which makes data unreadable but visible, steganography focuses on hiding the very presence of the message. In this approach, a cover image is selected and modified slightly to embed secret data while maintaining its visual quality. One of the commonly used methods is Least Significant Bit (LSB) substitution, where the least significant bits of pixel values are altered to store hidden information. Since these changes are minimal, the stego-image appears almost identical to the original image. Image steganography is widely used in secure communication, copyright protection, and covert data transmission due to its ability to provide secrecy without raising suspicion.

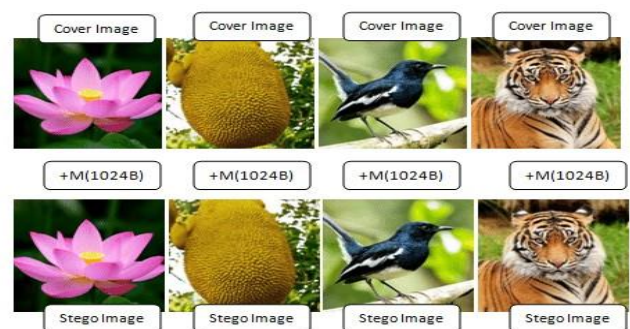


Fig -1: Image Steganography for Secure Data Hiding

1.2 AES Encryption for Enhanced Multimedia Security

Advanced Encryption Standard (AES) is a widely adopted symmetric key encryption algorithm known for its high security and efficiency. In multimedia data hiding systems, AES is used to encrypt the secret data before embedding it into the image. This ensures that even if an attacker successfully extracts the hidden data from the stego-image, the information remains protected and unreadable without the correct encryption key. AES operates on fixed-size data blocks and performs multiple rounds of substitution, permutation, and key mixing operations to achieve strong encryption. The combination of AES encryption with image steganography provides a dual-layer security mechanism, offering both data confidentiality and concealment. This makes the system highly suitable for protecting sensitive multimedia content against unauthorized access and cyber threats.

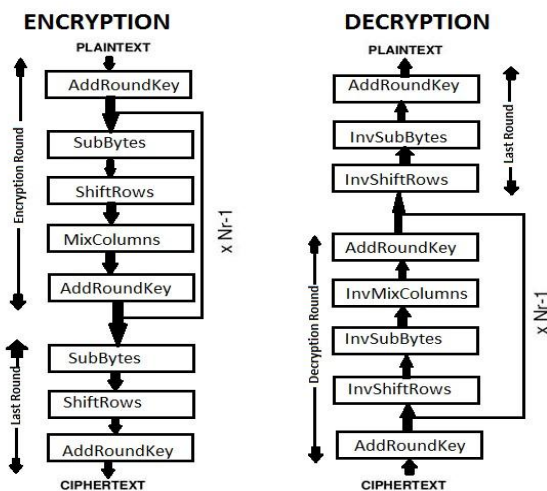


Fig -2: AES Encryption for Enhanced Multimedia Security

2. PROPOSED SYSTEM

The proposed system aims to provide a secure and efficient method for transmitting confidential multimedia data over insecure networks. It combines AES encryption with image steganography to ensure dual-layer security by protecting both the content and the existence of the secret data. In this system, the secret data is first encrypted using the Advanced Encryption Standard (AES). Encryption ensures that even if the hidden data is extracted by an unauthorized user, it remains unreadable without the correct key, thereby maintaining data confidentiality. After encryption, the encrypted data is embedded into a cover image using the Least Significant Bit (LSB) steganography technique. Since only the least significant bits of image pixels are modified, the visual quality of the image remains almost unchanged, making the hidden data difficult to detect. For data

extraction, the system requires the correct AES key and data length. The hidden encrypted data is extracted from the stego image and decrypted to recover the original secret content accurately and securely. The system also incorporates user authentication and access control. Users must register and receive admin approval before accessing the embedding and extraction features. This prevents unauthorized usage and enhances system security. The proposed system is implemented as a web-based application using the Django framework and supports multiple data formats such as text, image, audio, and video. This makes the system practical, scalable, and suitable for real-world secure communication applications.

2.1 System Architecture

The diagram illustrates the overall workflow of a secure multimedia data hiding system that integrates image steganography with AES encryption through a web-based interface. The process begins when the user uploads a cover image along with the secret data via a Django-based web interface. The uploaded data is forwarded to the stego module, where the secret information is first encrypted using the AES algorithm to ensure confidentiality. The encrypted data is then embedded into the cover image using the Least Significant Bit (LSB) technique, resulting in the generation of a stego image that visually appears unchanged from the original image. This stego image is securely stored in the media repository, and the AES key along with the embedded data length is sent to the authorized recipient through email notification. The system also includes an admin module that manages user access by approving or deactivating users to enhance security. Finally, the user can download and verify the stego image, ensuring secure transmission and controlled access to sensitive multimedia data.

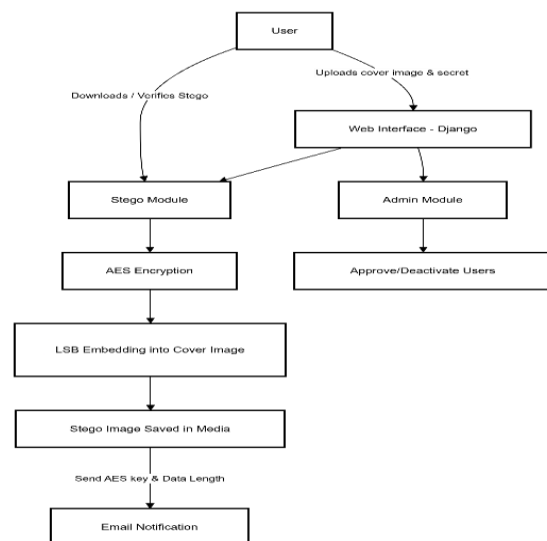


Fig -3: System Architecture

2.2 Web-Based Interface and User Management

The proposed system employs a web-based interface developed using the Django framework to provide secure and user-friendly interaction. This interface allows authenticated users to upload cover images and secret multimedia data for secure embedding. User access is strictly controlled through an admin module, where administrators can approve, monitor, or deactivate users based on system policies. This access control mechanism prevents unauthorized usage and enhances overall system reliability. The separation of user and admin roles ensures that sensitive operations, such as system configuration and user validation, are handled securely. By integrating user management into the architecture, the system maintains accountability, improves usability, and strengthens protection against malicious access attempts.

2.3 Secure Storage, Key Distribution, and Verification

After successful encryption and steganographic embedding, the generated stego image is securely stored in the system's media repository. To enable correct data extraction at the receiver end, essential information such as the AES encryption key and the length of the embedded data is transmitted securely through email notification to authorized users. This controlled key distribution mechanism ensures that only intended recipients can decrypt and recover the hidden information. Additionally, the system provides verification functionality that allows users to download and validate the stego image, confirming data integrity and authenticity. This architectural component ensures secure storage, controlled data access, and reliable retrieval of hidden multimedia content.

3. IMPLEMENTATION DETAILS

The proposed system is implemented as a secure, webbased application that integrates AES encryption with image steganography to achieve robust multimedia data protection. The system is developed using the Django framework, which handles user authentication, request processing, and rolebased access control through dedicated user and admin modules. Initially, an authenticated user uploads a cover image along with the secret multimedia data through the web interface. The uploaded data is validated for format and size constraints to ensure compatibility with the embedding process. Once validated, the secret data is passed to the encryption module, where the Advanced Encryption Standard (AES) algorithm is applied using a securely generated symmetric key. This encryption step converts the original data into an unreadable cipher format, ensuring confidentiality even if the hidden content is extracted by an unauthorized entity.

After encryption, the encrypted data is forwarded to the steganography module, where Least Significant Bit (LSB)

embedding is performed. In this process, the least significant bits of selected pixels in the cover image are modified to embed the encrypted data without causing perceptible changes to the image quality. The embedding algorithm carefully manages payload capacity and maintains image integrity by distributing the encrypted bits across the image pixels. The resulting stego image is then generated and stored securely in the media directory of the application with appropriate access restrictions. Simultaneously, essential metadata such as the AES key and the length of the embedded data are recorded and securely transmitted to the intended recipient via email notification.

On the administrative side, the admin module allows authorized administrators to approve or deactivate users, monitor system usage, and ensure that only trusted users can access the data hiding functionality. For data retrieval, the authorized user downloads the stego image and provides the correct AES key, after which the system performs LSB extraction to recover the encrypted data. The extracted cipher text is then decrypted using the AES algorithm to obtain the original multimedia content. This end-to-end implementation ensures dual-layer security by combining cryptographic strength with covert data hiding, making the system reliable, efficient, and suitable for secure multimedia communication applications.

4. RESULTS AND PERFORMANCE ANALYSIS

The experimental results demonstrate that the proposed secure multimedia data hiding system effectively achieves high confidentiality and imperceptibility. The generated stego images show minimal visual distortion when compared to the original cover images, indicating that the Least Significant Bit (LSB) embedding technique preserves image quality efficiently. Quantitative evaluation using parameters such as Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) confirms that the stego images maintain high PSNR values and low MSE, reflecting negligible degradation in image quality. The integration of AES encryption ensures strong data security, as the encrypted payload remains completely unreadable without the correct secret key, even if extraction is attempted. Performance analysis also indicates that the encryption, embedding, and extraction processes execute within acceptable time limits, making the system suitable for real-time or near real-time applications. Overall, the results validate that the proposed system provides a balanced trade-off between security, embedding capacity, and computational efficiency, making it reliable for secure multimedia communication.

5. CONCLUSIONS

The proposed system successfully demonstrates a secure and efficient approach for multimedia data protection by integrating image steganography with AES encryption. By encrypting the secret data before embedding it into a cover image, the system achieves a dual layer of security that

ensures both confidentiality and invisibility of the transmitted information. The use of the LSB embedding technique maintains high image quality while securely concealing encrypted data without noticeable visual distortion. Additionally, the web-based architecture with user and admin modules enhances usability, access control, and system reliability. Experimental evaluation confirms that the system provides strong security, efficient performance, and reliable data recovery, making it suitable for applications such as secure communication, digital watermarking, and confidential data sharing in modern multimedia environments.

FUTURE WORK

Although the proposed system provides effective security and reliable performance, several enhancements can be considered for future development. The system can be extended to support advanced steganographic techniques and adaptive embedding methods to further improve resistance against steganalysis attacks. In addition to image steganography, future work may include audio and video steganography to enable secure hiding of larger and more complex multimedia data. The use of stronger key management mechanisms and integration with public key cryptography or blockchain-based storage can enhance key security and traceability. Furthermore, incorporating machine learning-based attack detection and migrating the system to a cloud-based environment could improve scalability, automation, and real-time threat monitoring, making the solution more robust for large-scale secure multimedia applications.

ACKNOWLEDGEMENT

There are many people who helped us directly or indirectly to complete our project successfully. We would like to take this opportunity to thank one and all. We are extremely thankful and indebted to our supervisor, Mr. G. BHARATH Assistant Professor, Department of Information Technology, TKR College of Engineering and Technology, for his constant guidance, encouragement and moral support throughout the project. We are extremely thankful to Dr.N.satyanarayana , Head of the Department, Department of Information Technology, TKR College of Engineering and Technology, for the encouragement and support throughout the project. We are sincere thankful and gratitude to Dr. D. V. RAVI SHANKAR, Principal, TKR College of Engineering and Technology, for all the timely support and valuable suggestions during the period of our project. Finally, we would also like to thank all the faculty and staff of Information Technology Department who helped us directly or indirectly, parents and friends for their cooperation in completing the project work.

REFERENCES

- [1] N. Provos and P. Honeyman, "Hide and seek: An introduction to steganography," *IEEE Security & Privacy*, vol. 1, no. 3, pp. 32–44, 2003. DOI: 10.1109/MSECP.2003.1203220
- [2] J. Fridrich, "Applications of data hiding in digital images," *Proceedings of the IEEE International Conference on Information Technology*, pp. 1–6, 1999. DOI: 10.1109/ITNG.1999.845986
- [3] W. Stallings, "The Advanced Encryption Standard," *Cryptologia*, vol. 26, no. 3, pp. 165–188, 2002. DOI: 10.1080/0161-110291890885
- [4] A. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996. DOI: 10.1201/9781439821916
- [5] S. Katzenbeisser and F. A. P. Petitcolas, "Information hiding techniques for steganography and digital watermarking," *Artech House*, 2000. DOI: 10.1109/9780470605874