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 5, Issue 2, May 2025
Impact Factor: 7.67

Enhanced Data Security Using Video Steganography for Concealed Communication

Ms. A. Manthra[1], M. Ayshwarya[2], M. Iswarya[3], J. Maha Lakshmi[4]
Assistant Professor (M.E.), Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2,3,4]
Arasu Engineering college, Kumbakonam, India

Abstract: *This project introduces a highly secure method for protecting classified military information by combining Elliptic Curve Cryptography (ECC) and Least Significant Bit (LSB) video steganography. ECC ensures strong encryption with minimal computational overhead, while LSB embedding conceals encrypted data within video frames, making it imperceptible. The dual-layered security mechanism enhances data protection, making the system resilient to cryptographic and steganalytic attacks. The approach is well-suited for secure communication in defence, intelligence, and government sectors, maintaining video integrity while safeguarding sensitive information from cyber threats.*

Keywords: ECC, LSB steganography, encryption, cryptographic security, military data protection, cyber threats, secure communication, steganalysis resistance, video steganography

I. INTRODUCTION

This project presents a dual-layered security mechanism for military data protection by combining **Elliptic Curve Cryptography (ECC)** with **Least Significant Bit (LSB) video steganography**. ECC ensures strong encryption with minimal computational overhead, while LSB embedding conceals encrypted data within video frames, making it imperceptible. This approach enhances confidentiality by hiding encrypted messages in video pixels, ensuring secure transmission over untrusted networks. The method is ideal for real-time communications, providing lightweight security suitable for battlefield and defense systems. Experimental results confirm high imperceptibility and low computational overhead, making this framework effective against cyber espionage threats.

II. LITERATURE SURVEY

Secure Embedding of Speech Data into Digital Images Using Steganography, H. Vidhya, N. Shilpa, and S.M. Parvin (2025)

This study introduces a novel method for concealing speech data within images using steganography. The authors highlight the security of the incorporated speech by employing image encoding techniques. They propose a strategy that facilitates the secure transmission of speech data without compromising the image quality.

Data Hiding with Image Steganography and Cryptographic Algorithms, MS Hossen, MA Islam, and colleagues (2020)

This paper presents a comprehensive strategy for concealing data within images through advanced steganography methods integrated with the cryptographic algorithms AES and RC5. The researchers aim to enhance data security by encrypting the information before embedding it into the image files.

Enhanced LSB Steganography Technique for Color Images with Improved Capacity and Robustness, Zinia Sultana, Fatima Jannat, Sadman Sakib Saumik, Niloy Roy, Nishith Kumar Datta, and Muhammad Nazrul Islam(2017)

The authors detail an innovative Least Significant Bit (LSB) steganography technique particularly designed for color images. They focus on addressing common limitations observed in conventional LSB methods, such as capacity restrictions and susceptibility to attacks.

DOI: 10.48175/IJARSCT-26240

ISSN
2581-9429
IJARSCT

Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography—An Innovative Approach, M.M. Mahmoud and H.T. Elshoush(2022)

This investigation proposes a novel enhancement of the Least Significant Bit (LSB) technique for audio steganography through binary message size encoding. The authors' approach allows for a considerable increase in the capacity of audio data without sacrificing transparency, meaning the alterations to the audio file remain inaudible to human ears.

Secure Audio Cryptosystem Using Hashed Image LSB Watermarking and Encryption, Osama S. Faragallah and colleagues(2018)

The study introduces a secure audio cryptosystem that employs a hashed image as a watermarking technique in conjunction with the LSB method of data hiding. The authors emphasize the dual benefit of authentication and data confidentiality by concealing the encrypted audio payload within a host image. The hashing process enables the verification of the watermark's integrity and authenticity, adding another layer of security.

III. PROPOSED SYSTEM

Exsisting System

The Exsisting System uses Data Encryption Standard(DES) algorithm and asymmetric encryption techniques like RSA to encrypt the message and safely exchange the symmetric key.

RSA is used to encrypt the session key and DES used to encrypt the media streams in systems like secure video conferencing.

Digital rights management(DRM) systems also frequently employ asymmetric algorithms to restrict access to the decryption keys.

Drawbacks

- Key Distribution Challenges.
- Computational Inefficiency of Asymmetric Encryption.

Proposed Work

This system establishes a dual-layered security paradigm for safeguarding classified military communications by integrating Least Significant Bit (LSB) steganography with Elliptic Curve Cryptography (ECC). Leveraging LSB, encrypted data is seamlessly embedded into video frames, maintaining visual integrity while enabling discreet transmission across open or hostile networks. ECC fortifies this approach by employing compact yet highly secure encryption, ensuring optimal data protection within resource-constrained environments such as embedded military systems. The fusion of encryption and steganography enhances resilience against cryptographic attacks, cyber threats, and video processing techniques such as compression and cropping, guaranteeing that critical information remains concealed, secured, and inaccessible to unauthorized entities.

Advantages

- Dual-Layer Security
- High Undetectability
- Secure Key Distribution Mechanism

DOI: 10.48175/IJARSCT-26240

IV. SYSTEM ARCHITECTURE

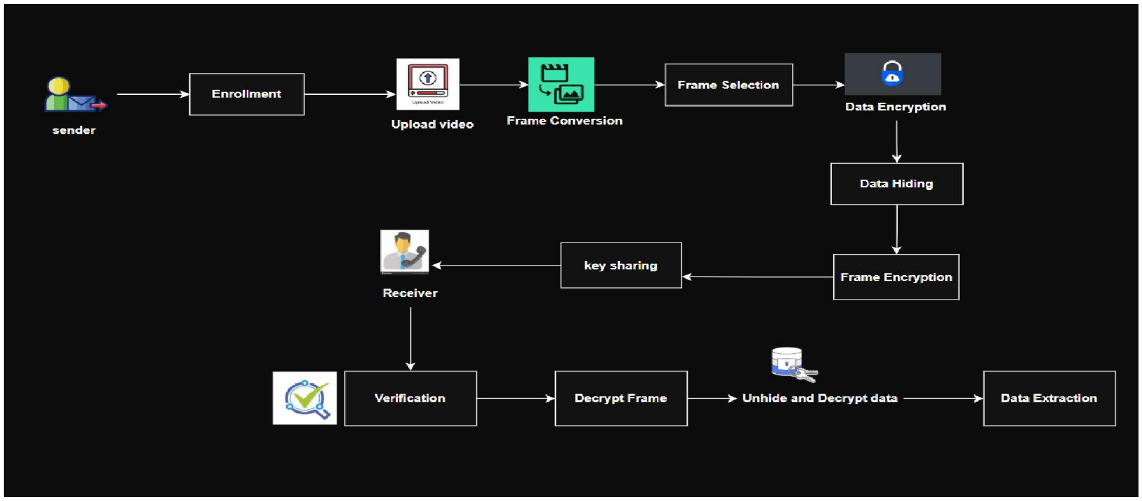

Figure 1 System Architecture

System Architecture Overview

- **Sender:** Initiates the process by providing data for secure transmission.
- **Enrollment:** Registers the sender to the system to authenticate communication.
- **Upload Video:** The sender uploads a video that will be used to hide the data.
- **Frame Conversion:** The uploaded video is converted into individual frames.
- **Frame Selection:** Suitable frames are selected for hiding the data.
- **Data Encryption:** The sensitive data is encrypted for secure embedding.
- **Data Hiding:** The encrypted data is embedded into the selected video frame(s).
- **Frame Encryption:** The modified frame containing hidden data is encrypted again for additional security.
- **Key Sharing:** Encryption keys are securely shared with the receiver.
- **Receiver:** The authorized recipient of the hidden data.
- **Verification:** Validates the identity of the receiver before decryption.
- **Decrypt Frame:** The encrypted frame is decrypted to access the hidden data.
- **Unhide and Decrypt Data:** The hidden data is extracted and decrypted.
- **Data Extraction:** Final retrieval of the original data for use by the receiver.

V. ALGORITHMS

Elliptic Curve Cryptography (ECC):

Elliptic Curve Cryptography (ECC) is a powerful public-key encryption technique that offers strong security with relatively small key sizes, making it efficient for resource-constrained environments. Unlike traditional methods like RSA, ECC leverages mathematical properties of elliptic curves to provide secure encryption and decryption. Its lightweight nature makes it ideal for military applications, embedded systems, and mobile devices where computational efficiency is crucial. ECC ensures data remains protected even if intercepted, as unauthorized access requires solving complex mathematical problems beyond modern computing capabilities.

Least Significant Bit (LSB) Steganography:

Least Significant Bit (LSB) steganography is a technique used to conceal sensitive information within digital media files, such as images or videos. By subtly modifying the least significant bits of pixel values, LSB embedding allows data to be hidden in a way that is imperceptible to the human eye. Since these alterations do not significantly affect the visual quality of the media, the steganographic message remains undetectable under normal observation. This method is particularly useful for covert communication, ensuring encrypted data can be transmitted discreetly across untrusted networks without raising suspicion.

VI. MODULES

Enrolment and Data Sharing:
Users (senders and receivers) are assigned unique IDs and credentials, with ECC generating secure public-private key pairs for encrypted data exchange, ensuring controlled access.

Video Upload:
Users submit a compatible video file to act as a cover for sensitive data, maintaining confidentiality without degrading visual quality.

Frame Conversion and Selection:
The video is segmented into frames, with selected ones chosen based on clarity and stability to ensure effective data concealment without distortion.

Data Encryption:
Sensitive data is encrypted using ECC, which offers strong security with small key sizes and ensures only authorized recipients can decrypt the information.

Data Hiding:
Encrypted data is embedded into selected video frames using LSB steganography, modifying pixel values subtly to store information without affecting visual integrity.

Frame Encryption:
After embedding, video frames themselves are encrypted, adding another layer of protection against unauthorized extraction or alteration.

Keys Sharing:
ECC cryptographic keys are securely shared, with only the sender's public key distributed while the receiver uses their private key to derive the shared secret.

Key Verification and Data Extraction:
The receiver verifies the sender’s identity and decrypts the video frames, reversing the LSB embedding to retrieve the encrypted message and applying ECC decryption to obtain the original data.

VII. CONCLUSION

The proposed system integrates Elliptic Curve Cryptography (ECC) with Least Significant Bit (LSB) steganography to ensure military data remains both encrypted and hidden. ECC provides strong security, while LSB discreetly embeds encrypted information in video frames, making detection nearly impossible. This dual-layered approach enhances confidentiality, integrity, and resilience against cyber threats. With lightweight cryptographic operations and imperceptible data concealment, the system is well-suited for deployment in high-risk and resource-constrained environments, ensuring secure defense communications.

REFERENCES

[1] H. Vidhya, N. Shilpa, and S. M. Parvin, "Secured Speech Data Hiding using Steganography of Images," ResearchGate, accessed Apr. 29, 2025.

DOI: 10.48175/IJARSCT-26240

ISSN
2581-9429
IJARSCT

[2] I. Haverkamp and D. K. Sarmah, "Evaluating the merits and constraints of cryptography-steganography fusion: a systematic analysis," International Journal of Information Security, vol. 23, pp. 1-12, 2024.

[3] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image steganography using LSB and hybrid encryption algorithms," Applied Sciences, vol. 13, no. 1, p. 12345, 2023.

[4] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB using binary message size encoding for high capacity, transparent and secure audio steganography—an innovative approach," IEEE Access, vol. 10, pp. 1-10, 2022.

[5] M. A. Mahmood and T. Tabassum, "A hybrid cryptographic data security system utilizing fuzzy vault key," in 2021 IEEE International …, 2021.

[6] M. S. Hossen, M. A. Islam, and T. Khatun, "A new approach to hiding data in the images using steganography techniques based on AES and RC5 algorithm cryptosystem," Smart Electronics, 2020.

[7] P. P. Bandekar and G. C. Suguna, "LSB based text and image steganography using AES algorithm," in 2018 3rd International Conference …, 2018.

[8] O. S. Faragallah, "Secure audio cryptosystem using hashed image LSB watermarking and encryption," Wireless Personal Communications, vol. 100, no. 1, pp. 1-13, 2018. 67

[9] Z. Sultana, F. Jannat, S. S. Saumik, and N. Roy, "A new approach to hide data in color image using LSB steganography technique," Electrical Information, vol. 2017, pp. 1-6, 2017.

[10] R. Jabi, P. Patel, and D. Dubey, "An efficient secure data transmission based on visual cryptography," in 2016 International Conference on …, 2016