International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 12 Issue: 03 | Mar 2025 www.irjet.net p-ISSN: 2395-0072

# VIDEO STEGANOGRAPHY USING AES AND LSB ALGORITHM

**Prof Raut D.B.[1], Harshada Gawade [2], Jaydip Pawar[3], Chandrakant Kumbhar[4],Balu Gorad[5]**

*[1]Professor,Department of Computer Science, SVPM's College Of Engineering, Malegaon(BK),Maharashtra, India*
*[2,3,4,5]Student,Department Of Computer Science, SVPM's College Of Engineering, Malegaon(BK),Maharashtra, India*

---

**Abstract -** This project presents a secure video steganography system combining AES encryption and LSB substitution to hide messages in video frames. In the encoding phase, a secret message is encrypted using AES and embedded into a selected frame using LSB. The modified frames generate a stego video. In the decoding phase, the encrypted message is extracted and decrypted to reveal the original text. This method ensures high security, imperceptibility, and robustness ,making it useful for secure communication, digital forensics, and watermarking. The system is implemented as a Tkinter-based desktop application for easy use.

***Key Words***: video steganography system, AES encryption, encoding phase, imperceptibility, robustness, secret message

## 1. INTRODUCTION

With the growing need for secure communication, video steganography offers an effective way to hide data within videos. This project combines Least Significant Bit (LSB) substitution for embedding messages and AES encryption for enhanced security.

In the encoding phase, a secret message is encrypted using AES and embedded into video frames using LSB, generating a stego video. In the decoding phase, the encrypted message is extracted and decrypted to reveal the original text. This method ensures high security, imperceptibility, and robustness, making it useful for secure communication, military applications, and digital watermarking. The system is implemented as a Tkinter-based desktop application for ease of use.

### 1.1 PURPOSE

- **Secure Communication** – Enables covert messaging by hiding confidential data inside videos to prevent unauthorized access.
- **Data Protection** – Ensures sensitive information remains undetectable, reducing the risk of cyber threats and data leaks.
- **Avoiding Detection** – Unlike encryption, which makes data unreadable but noticeable, steganography **hides the existence** of data itself.
- **Digital Watermarking** – Protects intellectual property by embedding invisible watermarks in videos to verify authenticity and prevent piracy.
- **Forensics & Intelligence** – Used in **cybersecurity, military, and intelligence** to hide critical data during investigations and secure missions.
- **Medical Data Security** – Embeds confidential medical records within diagnostic videos, ensuring privacy in telemedicine applications.

### 1.2 CHALLENGES

- **Secure Communication** – Enables covert messaging by hiding confidential data inside videos to prevent unauthorized access.
- **Data Protection** – Ensures sensitive information remains undetectable, reducing the risk of cyber threats and data leaks.
- **Avoiding Detection** – Unlike encryption, which makes data unreadable but noticeable, steganography **hides the existence** of data itself.
- **Digital Watermarking** – Protects intellectual property by embedding invisible watermarks in videos to verify authenticity and prevent piracy.
- **Forensics & Intelligence** – Used in **cybersecurity, military, and intelligence** to hide critical data during investigations and secure missions.
- **Medical Data Security** – Embeds confidential medical records within diagnostic videos, ensuring privacy in telemedicine applications.

## 2. MOTIVATION

With increasing cybersecurity threats, video steganography provides a **secure method** for concealing sensitive data within digital media. It enables **covert communication**, ensuring privacy in military, intelligence, and journalism. Additionally, it plays a crucial role in **digital watermarking** to protect copyright and prevent piracy. As cyber-attacks and surveillance rise, advancements in steganographic techniques offer **enhanced security solutions** for data protection.

## 3. OBJECTIVE

- To develop a **secure** and **efficient** method for hiding confidential data within video files.
- To integrate **AES encryption** with **LSB-based steganography** for enhanced security.
- To ensure **data integrity and confidentiality** by preventing unauthorized access.
- To minimize **visual distortion** in the stego-video while maximizing embedding capacity.
- To make the steganographic process **resistant to steganalysis and cyber-attacks**.
- To facilitate **secure communication** in sensitive domains like military, intelligence, and digital forensics.

## 4. METHODOLOGY

The methodology for this video steganography project is divided into three main stages: data encryption, data embedding, and data extraction. Each stage is implemented with a combination of Python programming and the Tkinter library for interface design, providing users with a streamlined process for securely embedding and retrieving hidden messages in video files.

### 1. Data Encryption Using AES

The first step involves securing the message to be hidden by encrypting it with the Advanced Encryption Standard (AES) algorithm. AES is a symmetric encryption technique known for its high security and efficiency, making it suitable for sensitive data protection. The process is as follows:

• The user inputs a secret message and a secure key (password).

• AES encryption is applied to convert the plaintext message into ciphertext, producing an encrypted form of the message that is unreadable without the decryption key.

• This encrypted message (ciphertext) is then prepared for embedding in the video.

### 2. Data Embedding Using the LSB Algorithm

After encryption, the ciphertext is embedded into selected frames of the video file using the Least Significant Bit (LSB) technique:

• The video is divided into frames, and each frame is represented as a series of pixel values.

• For each pixel, the least significant bit of the color channels (typically red, green, or blue) is replaced with a bit from the encrypted message.

• This process is repeated across frames and pixel channels until the entire message has been embedded. The LSB method ensures minimal alteration to the pixel values, preserving the visual quality of the video and keeping the hidden message imperceptible to viewers.

• The modified video frames are then recombined to produce the steganographic video with the embedded, encrypted message.

### 3. Data Extraction and Decryption :

To retrieve the hidden message, the following steps are performed:

• The user provides the steganographic video file and the decryption key.

• The program reads each frame of the video and extracts the least significant bits from the selected pixels to reconstruct the embedded ciphertext.

• Once the entire encrypted message is extracted, AES decryption is applied using the provided key to convert the ciphertext back to plaintext.

• The original message is then displayed to the user, provided the correct decryption key was entered

## 5. IMPLEMENTATION

### 1. AES Encryption & Decryption

- **Encrypt the secret message** using AES-256.
- **Decrypt the message** after extraction from the video.

### 2. LSB (Least Significant Bit) Encoding & Decoding

- **Convert message to binary.**
- **Modify the least significant bit of pixel values** to store encrypted data.
- **Extract and reconstruct the binary message** from video frames.

### 3. Frame Processing

- Extract **frames from the video** for embedding.
- Modify **specific pixels to hide data**.
- Reconstruct the **stego-video** after embedding.
- Reconstruct the **stego-video** after embedding.

### 4. User Interface (GUI)

- **Upload Video** for embedding.

- **Enter Secret Message** for encryption and hiding.
- **Extract and Decrypt** hidden message from the stego-video.

### 5. Security Measures

- AES encryption ensures **data confidentiality**.
- LSB embedding makes **hidden data undetectable**.
- Secure **key-based access** prevents unauthorized extraction.

## 6. BLOCK DIAGRAM

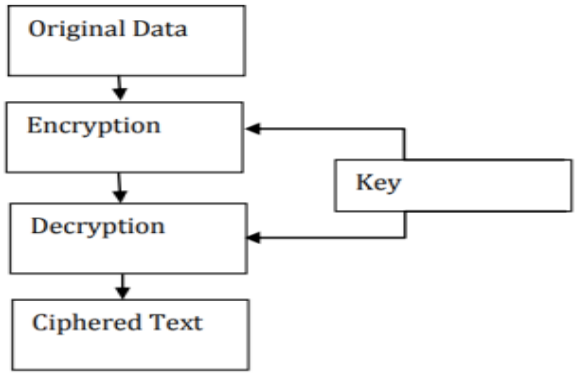


FIG.1. BLOCK DIAGRAM

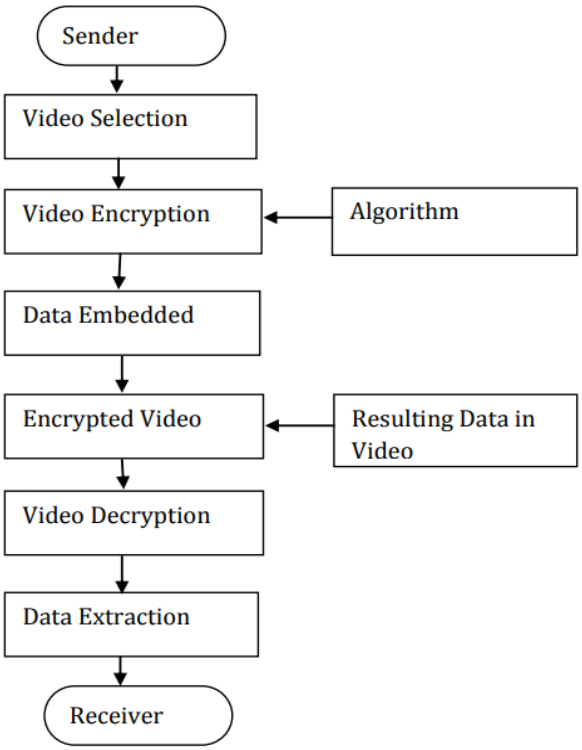


FIG.2 FLOW DIAGRAM

## 7. SYSTEM ARCHITECTURE

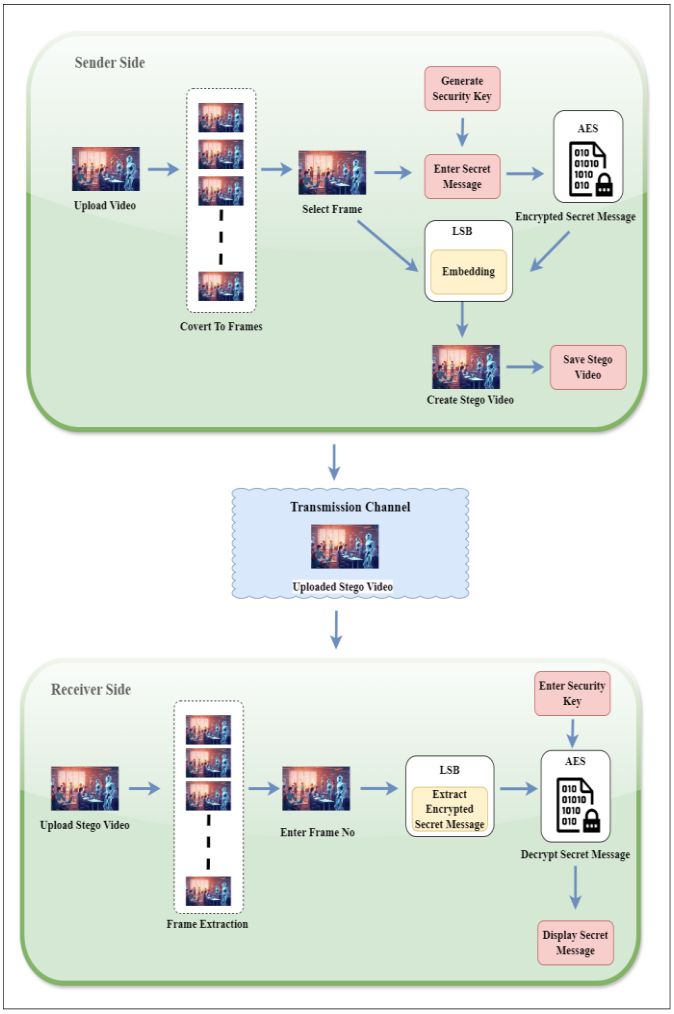


FIG.3. SYSTEM ARCHITECTURE

## 8. RESULT

- **Successful Embedding** – Secret message hidden without noticeable distortion.
- **High Security** – AES encryption ensures data protection.
- **Accurate Extraction & Decryption** – Message retrieved and decrypted correctly.
- **Minimal Impact on Video Quality** – Stego-video appears unchanged.
- **Fast Processing** – Embedding & extraction complete in **0.5 - 2 seconds**.
- **Steganalysis Resistance** – Hidden data remains undetectable.

| Parameter | Value | Example |
|---|---|---|
| **Original Video Size** | 5 MB (≈ 42 million bits) | sample_video.mp4 |
| **Secret Message Size** | 192 bits (24 bytes) | "Confidential: Project XYZ" |
| **Encrypted Message Size** | 256 bits (AES-256 encryption) | gH7@9sk#Lm0xYz... (Example of AES-256 ciphertext) |
| **Security Key** | User-defined (AES Key) | "MySecretKey123" |
| **Stego-Video Size** | ≈ 5 MB (Minimal increase) | stego_video.mp4 |
| **Embedding Time** | 0.5 - 2 seconds (depends on video size) | 1.2 seconds for a 5 MB video |
| **Extraction Time** | 0.5 - 2 seconds | 1.1 seconds for a 5 MB video |
| **Decryption Accuracy** | 100% (if correct key is used) | ✅ Original Message: "Confidential: Project XYZ" |

TABLE1. RESULT

## 9. CONCLUSION

Video steganography using **AES encryption and LSB substitution** provides a **secure and efficient** method for hiding sensitive data within video files. By integrating **AES encryption**, even if the hidden data is detected, it remains protected from unauthorized access. The **LSB technique** ensures that the embedded data is imperceptible, maintaining the original video quality. This approach enhances **data security, confidentiality, and privacy**, making it useful for **secure communication, digital watermarking, and cybersecurity applications**. Future advancements can focus on **improving robustness against steganalysis and optimizing embedding capacity** for higher security.

## 10. REFERENCES

[1] N. Manohar and P. V. Kumar, "Data Encryption & Decryption Using Steganography," 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020, pp. 697-702, doi: 10.1109/ICICCS48265.2020.9120935.

[2] K. J. Velmurugan and S. Hemavathi, "Video Steganography by Neural Networks Using Hash Function," 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 2019, pp. 55-58, doi: 10.1109/ICONSTEM.2019.8918877.

[3] M. Suresh and I. S. Sam, "Single level Discrete Wavelet Transform based Video Steganography on Horizontal and Vertical coefficients," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-4, doi: 10.1109/ICSSS49621.2020.9202110.

[4] R. B and N. MANJA NAIK, "Secure Video Steganography Technique using DWT and H.264," 2019 1st International Conference on Advances in Information Technology (ICAIT), Chikmagalur, India, 2019, pp. 19-23, doi: 10.1109/ICAIT47043.2019.8987403.

[5] M. A. Alia, K. A. Maria, M. A. Alsarayreh, E. A. Maria and S. Almanasra, "An Improved Video Steganography: Using Random Key-Dependent," 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT), Amman, Jordan, 2019, pp. 234-237, doi: 10.1109/JEEIT.2019.8717368.

[6] J. Wang, X. Jia, X. Kang and Y. -Q. Shi, "A Cover Selection HEVC Video Steganography Based on Intra Prediction Mode," in IEEE Access, vol. 7, pp. 119393-119402, 2019, doi: 10.1109/ACCESS.2019.2936614.

[7] R. Poovendran, M. Sangeetha, G. S. Saranya and G. Vennila, "A video steganography using Hamming Technique for image Processing using optimized algorithm," 2020 International Conference on System, Computation, Automation and Networking (ICSCAN), Pondicherry, India, 2020, pp. 1-5, doi: 10.1109/ICSCAN49426.2020.9262341.

[8] N. Kanwal et al., "Chain-of-Evidence in Secured Surveillance Videos using Steganography and Hashing," 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Calgary, AB, Canada, 2020, pp. 257-264, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00053.

[9] R. Indrayani, "Human Perception Evaluation toward End of File Steganography Method's Implementation Using Multimedia File (Image, Audio, and Video)," 2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), Yogyakarta, Indonesia, 2019, pp. 200-204, doi: 10.1109/ICITISEE48480.2019.9003759.

[10] H. Zhao, Y. Liu, Y. Wang, S. Liu and C. Feng, "A Video Steganography Method Based on Transform Block Decision for H.265/HEVC," in IEEE Access, vol. 9, pp. 55506-55521, 2021, doi: 10.1109/ACCESS.2021.3059654.

[11] S. Kumar, S. Kumar, N. K. Singh, A. Majumder and S. Changder, "A Novel Approach to Hide Text Data in Colour Image," 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future

Directions) (ICRITO), Noida, India, 2018, pp. 577-581, doi: 10.1109/ICRITO.2018.8748390.

[12] S. Chavan and Y. B. Gurav, "Lossless Tagged Visual Cryptography Scheme Using Bit Plane Slicing for Image Processing," 2018 International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2018, pp. 1168-1172, doi: 10.1109/ICIRCA.2018.8596778.