e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:06/Issue:11/November-2024 Impact Factor- 8.187 www.irjmets.com

VIDEO STEGANOGRAPHY USING AES AND LSB

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

*[1]Prof., Computer Engineering, SVPM's College Of Engineering Malegaon(BK), Pune, Maharashtra, India.

*[2,3,4,5]UG Students, Computer Engineering, SVPM's College Of Engineering Malegaon(BK), Baramati, Maharashtra, India.

ABSTRACT

With the rapid growth of digital communication, safeguarding confidential information has become paramount. Video steganography provides a viable solution for secure data transmission by concealing sensitive information within video files, leveraging the large data capacity and low perceptibility of video media. This project explores a video steganography approach that combines the Least Significant Bit (LSB) technique for data embedding with the Advanced Encryption Standard (AES) for data encryption, providing an additional layer of security. By encrypting the data with AES before embedding it into the video frames, the system ensures that even if the hidden data is discovered, it remains unintelligible without the decryption key. Implemented using Python and Tkinter for a user-friendly interface, the application allows users to securely embed and retrieve data within video files. The effectiveness of the method is evaluated based on criteria such as imperceptibility, robustness, and efficiency, demonstrating that the combination of AES encryption and LSB-based steganography provides a robust solution for secure, covert data transmission. This dual-layered approach enhances the confidentiality of sensitive data, meeting the demand for more secure communication methods in today's digital landscape.

Keywords: Data Security, Data Embedding, Encryption, Secure Data Transmission, Confidentiality.

I. INTRODUCTION

The primary aim of video steganography is to embed hidden messages within a video file in such a way that they remain imperceptible to the human eye. Among various methods, the Least Significant Bit (LSB) technique is one of the most widely used for embedding data in digital media. It operates by replacing the least significant bits of pixel values with bits from the secret message, ensuring minimal alteration to the original media.

To further enhance security, video steganography can be combined with encryption algorithms, such as the Advanced Encryption Standard (AES). By encrypting the hidden message before embedding it in the video, the system ensures that even if the embedded data is detected, it cannot be accessed without the correct decryption key. This combination of encryption and steganography provides a dual-layered approach to data security, making it an effective solution for sensitive data transmission. This project focuses on the implementation of video steganography using the LSB technique and AES encryption, creating a secure environment for embedding and retrieving data within video files. Python and Tkinter are used to develop a user-friendly interface, allowing users to seamlessly encrypt, embed, and extract hidden messages. Through evaluation of metrics like imperceptibility, robustness, and data capacity, this project aims to demonstrate the viability of combining steganography and encryption to meet modern data security demands in digital communication.

II. 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.

III. SYSTEM ARCHITECTURE

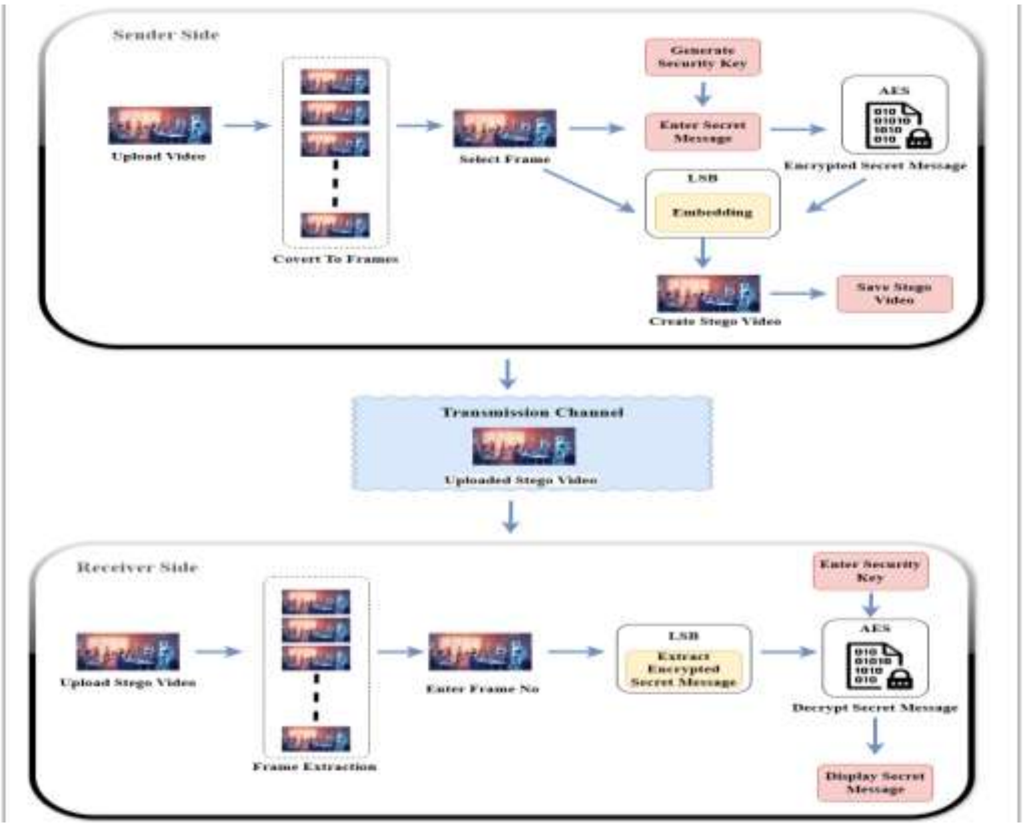

Fig 1: System Architecture

IV. PROPOSED SYSTEM

The proposed video steganography system provides a secure method to hide sensitive information within video files by combining the Least Significant Bit (LSB) embedding technique with AES encryption. The system operates in three stages:

1. **Message Encryption**: The user inputs a message and an encryption key, which is used by the AES module to generate encrypted ciphertext, ensuring data security even if the embedded content is detected.
2. **Data Embedding**: The encrypted message is embedded in the least significant bits of video frame pixels using the LSB technique. This keeps the changes imperceptible, preserving the video's quality.
3. **Data Extraction and Decryption**: For retrieval, the LSB extraction module recovers the hidden encrypted message, and AES decryption converts it back to plaintext using the correct key.

A user-friendly Tkinter interface supports the entire process, guiding users from encryption to embedding and extraction. This system enhances data confidentiality and provides an accessible, secure way to transmit hidden messages within video files.

V. CONCLUSION

Video steganography presents a powerful method for secure communication by concealing information within video files, making it highly effective for covert data transmission. This project implemented a video steganography system combining the Least Significant Bit (LSB) technique for embedding and AES encryption for enhanced security. By encrypting the message before embedding, the system ensures that even if the hidden data is discovered, it remains protected and unreadable without the correct decryption key.

Through evaluation, the system demonstrated robust imperceptibility, preserving video quality while successfully hiding data, as well as strong security against unauthorized access. This one-layer approach, using steganography shows promise for applications in secure digital communication, where data integrity and confidentiality are critical. Future work may involve improving robustness against compression and exploring real-time applications, further advancing the potential of video steganography as a secure, adaptable communication tool.

ACKNOWLEDGEMENTS

We take this opportunity to thank our project guide Prof. Raut D.B. and Head of the Department Prof. Khalate Y.R. and Honorable Principal Prof. Dr. Mukane S.M. for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this project report. We are also thankful to all the staff members of the Department of Computer Engineering of SVPM's College of Engineering, Malegaon (Bk) for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important book.

VI. 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.