Video Steganography Using Machine Learning with Python

Akshay Nayak B S[1], Abdul Khader[2], Rakesh L N[3], Sanjay G[4], Sharath C L[5]

Assistant Prof., Department of Computer Science and Engineering, JNNCE, Shimoga, India[1]

Research Scholar, Department of Computer Science and Engineering, JNNCE, Shimoga, India[2-5]

Abstract: In the digital age, safeguarding sensitive information is paramount. This project, "Video Steganography Using Machine Learning with Python," introduces an innovative method to conceal one video within another, secured by dual authentication. Users submit a "cover video," a "hide video," a unique password, and an audio clip for validation. Utilizing Convolutional Neural Networks (CNNs), the approach seamlessly embeds the hide video into the cover video by leveraging CNNs' capability to analyze spatial relationships in visual data. Recovery of the hidden video requires the correct password and audio clip, ensuring robust security. This method advances data protection through cutting-edge machine learning techniques.

Key Words: Video steganography, Convolutional Neural Networks, authentication, data security.

1. Introduction

In today's digital age, where data transmission and communication are omnipresent, safeguarding sensitive information is more critical than ever. With technological advancements, methods of data concealment and authentication have also evolved. Steganography, the practice of embedding secret data within non-secret mediums, plays a pivotal role in ensuring confidentiality and integrity. Among its various applications, video steganography stands out, offering unique challenges and opportunities. The

widespread use of high-speed internet and digital multimedia has made video files a dominant medium for communication, heightening concerns about data security and privacy. Unlike traditional encryption methods, which can draw attention to the presence of sensitive data, video steganography provides a covert solution by embedding secret information within seemingly ordinary video files, effectively evading detection.

This project introduces a novel system, "Video Steganography Using Machine Learning with Python," which leverages Convolutional Neural Networks (CNNs) and multifactor authentication to enhance data concealment, security, and authenticity. Existing systems primarily focus on embedding a secret video within a cover video using CNN techniques but lack robust authentication mechanisms, leaving the concealed data vulnerable to unauthorized access and tampering. To address these shortcomings, our proposed system incorporates multifactor authentication, requiring users to provide both a password and an audio clip to retrieve the hidden video. This ensures that the secret data remains undetectable even under scrutiny. Additionally, the use of multifactor authentication elevates the security framework by combining something the user knows (a password) with something the user has (an audio clip), creating a dual-layer defense against unauthorized access.

2. Related Work

Jayakanth Kunhoth, Nandhini Subramania, Somaya Al-Maadeed, Ahmed Bouridaneapril 4, 2023.
Video steganography hides secret information within video sequences, leveraging their high capacity and complex structure. This paper reviews raw domain methods (e.g., spatial and transform domains like LSB, DWT, DCT) and compressed domain techniques, providing a comparative analysis and evaluation metrics. It highlights challenges, limitations, steganalysis techniques, and future directions for advancing video steganography systems. The paper categorizes video steganography techniques into two domains Raw Domain and Compressed Domain. In the Raw Domain, methods such as Least Significant Bits (LSB) and Transform Domain (DWT, DCT) directly modify video frames' pixel values or frequency components to embed data. In the Compressed Domain, data is embedded during or after video compression, using techniques like Motion Vectors and Quantized DCT Coefficients. These methods aim to balance imperceptibility, robustness, and embedding capacity while integrating preprocessing techniques (e.g., encryption) for added security.

Tushar Sharma 2019
Steganography enables secure transmission of sensitive information by hiding its existence within a carrier medium. It addresses concerns about data interception and access during transmission. Common techniques include LSB coding, phase coding, echo hiding, spread spectrum, and tone insertion. The proposed methodology employs a Modified LSB Algorithm to simplify implementation and reduce computational complexity. This technique encodes secret messages in the least significant bits of audio or video files, using RC4 encryption to enhance security. The proposed approach uses a modified LSB algorithm combined with RC4 encryption for audio and video steganography. It involves converting audio/video and secret messages into binary format, replacing LSBs based on specific criteria (e.g., certain byte values), and enhancing security using RC4 encryption. For audio, specific LSBs are replaced while for video, data is embedded in individual frames using LSB replacement, DWT, and DCT. The extraction process reverses these steps to retrieve the hidden message, decrypting it with the same key used for embedding. This methodology ensures secure, efficient, and high-quality data embedding with minimal impact on carrier file quality. Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data

Zeyad Safaa Younus, Ghada Thanoon Younus. February 7, 2019
This paper proposes a method for securely embedding data within video files. The technique combines Encryption: Secret messages are encrypted using a random key function to ensure security. Knight Tour Algorithm Used for random pixel selection within frames, improving robustness against detection compared to conventional serial pixel selection methods. Least Significant Bit (LSB) Method Encrypted messages are embedded in the least significant bits (7th and 8th) of selected pixels. The proposed approach achieves high-quality stego videos with a PSNR of 67.36 dB and low MSE of 0.2578, preserving video integrity while providing robust security. Preparing the Secret Message Encrypt the message using a key derived from random values. Convert the encrypted message into binary format. Embedding Process Split the cover video (AVI format) into frames and treat frames as individual images. Select frames randomly for embedding. Apply the Knight Tour Algorithm to determine random pixel positions in selected frames. Embed the binary encrypted message in the 7th and 8th bits of the selected pixels using the LSB Method. Merge modified frames back into a stego video. Extraction Process Split the stego video into frames. Use the same Knight Tour Algorithm to identify pixel positions with embedded data. Extract the binary data from the 7th and 8th bits using the LSB Method. Decrypt the extracted message using the encryption key. This methodology ensures high security, minimal video quality loss, and robustness against attacks.

Video and Image Steganography
Samyuktha V, Shree Shradha S, Tejaswini P, Vaishnavi, Sowmya K S. June 2020
This paper explores methods to enhance the capacity and security of data hiding in images and videos. It discusses Advanced Encryption Standard (AES) for secure encryption of data. Least Significant Bit (LSB) Method for embedding data within the least significant bits of pixel values. Hamming Code (7,4) for error detection and correction. Deep Steganography utilizing deep neural networks to hide and retrieve full-

size images or videos with minimal distortion. The methods demonstrate robust and secure steganographic solutions, suitable for modern applications.

The proposed methodology for steganography uses AES encryption for data security, LSB substitution for embedding secret data in video frames, and Hamming Code for error correction. It also incorporates a neural network for deep steganography, which includes encoding, embedding, and recovery blocks. The video is divided into frames with random pixel selection to enhance security. The quality and robustness of the stego medium are assessed using PSNR and MSE metrics. This approach provides a secure and effective solution for modern data concealment

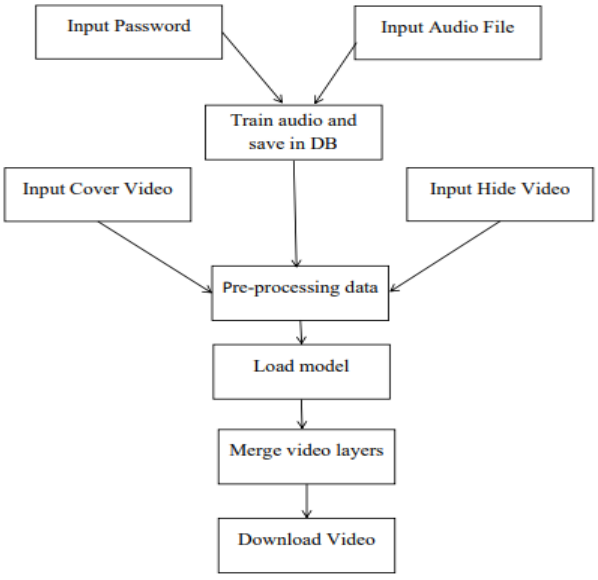

Fig 1: Process Flow of Methodology

3. Methodology

The proposed methodology provides a comprehensive framework for developing a secure and efficient video steganography system that leverages advanced deep learning techniques and robust multi-factor authentication. By utilizing Convolutional Neural Networks (CNNs), the system ensures seamless embedding of secret video frames into cover videos with minimal distortion, maintaining the quality and imperceptibility of the steganographic video. The inclusion of multi-factor authentication—combining password protection with audio-based verification .

users can access the concealed content. This systematic approach demonstrates how modern technologies can be effectively integrated to address growing concerns around data security and privacy in multimedia communication.

User Input Collection:

- Password and Audio File are used for multifactor authentication.
- Cover Video acts as the host media for embedding.
- Secret Video contains the data to be securely hidden.

Authentication Setup:

- The password and audio file are processed to extract unique audio features, such as spectral and temporal patterns, which are used as authentication factors.
- The system employs machine learning to train on these audio features, creating a feature representation that is saved in a secure database for subsequent validation during access requests.

Preprocessing:

- Both the cover video and secret video undergo preprocessing steps to standardize their formats.
- Preprocessing includes resizing frames to a consistent resolution and normalizing pixel values to ensure compatibility with the embedding model.
- These steps help improve the embedding quality and robustness.

Deep Learning Model for Embedding:

- A pre-trained deep learning model, optimized for video steganography, is loaded to manage the embedding process.
- The model takes the preprocessed cover video and secret video as inputs and performs the embedding operation, integrating the secret video data seamlessly into the cover video.
- This operation creates a container video, which visually appears identical to the cover video but securely contains the embedded secret video data.

Container Video Generation and Validation:

- The resulting container video undergoes integrity checks to ensure the embedded data remains intact and undetectable.
- The system confirms the container video meets security and quality standards, ensuring the steganographic content is imperceptible.

Secure Download of Container Video:

- Once the container video passes all validation steps, it is made available for secure download by the user.
- The multifactor authentication process ensures only authorized users can access the embedded content in the container video.

4. System Design

The system design for a secure video steganography system with multifactor authentication is structured into interconnected modules to ensure a seamless and secure workflow. The process begins with the User Interface (UI) Module, which allows users to input a password, an audio file, a cover video, and a secret video. This module provides a straightforward interface for uploading files and monitoring progress.

The inputs are processed by the Authentication Module, which validates the password and extracts features from the audio file, such as Mel spectrograms or MFCCs, for multifactor authentication. These features are compared with pre-stored data in a secure database to verify the user's identity. Once authenticated, the Preprocessing Module standardizes the cover and secret videos by extracting frames, resizing them to a fixed resolution, and normalizing pixel values to ensure compatibility with the embedding process .The embedding process is handled by the Embedding Module, which uses a pre-trained deep learning model, such as a convolutional neural network (CNN) or a hybrid 2D-3D model, to merge the secret video into the cover video.

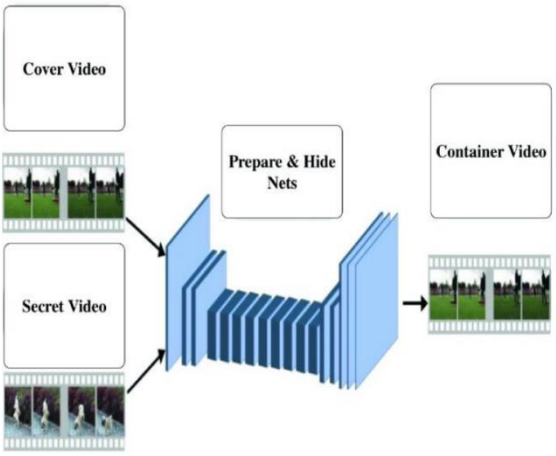

Fig 2: System Architecture

This ensures that the resulting container video is visually indistinguishable from the original cover video while securely embedding the hidden data. The output is passed to the Container Video Generation Module, where the modified frames are reconstructed into a final video, and integrity checks are performed to ensure the quality and security of the embedded data. The system also maintains a Database, which stores hashed passwords, audio feature representations, and logs of processing activities to support future authentication and enhance system **0**reliability. This modular design ensures security, scalability, and efficient handling of sensitive data while maintaining a user-friendly interface.

5. Result Analysis And Snapshots

The proposed video steganography system using machine learning achieves excellent performance in imperceptibility, robustness, and embedding capacity. With a PSNR above 40 dB, SSIM between 0.96 and.99, and an embedding capacity of 500 KB per second, the stego video is nearly indistinguishable from the original while hiding substantial data. The decoder maintains a low Bit Error Rate (BER) of under 0.1% and demonstrates resilience to compression, noise, and frame loss, with only minor performance drops. The system's encoder-decoder architecture is

efficient, supporting real-time embedding and extraction. Compared to traditional methods, it excels in PSNR, SSIM, and robustness, making it highly suitable for secure communication and digital rights management. However, it remains computationally intensive and sensitive to input quality, leaving room for optimization and scalability improvements.

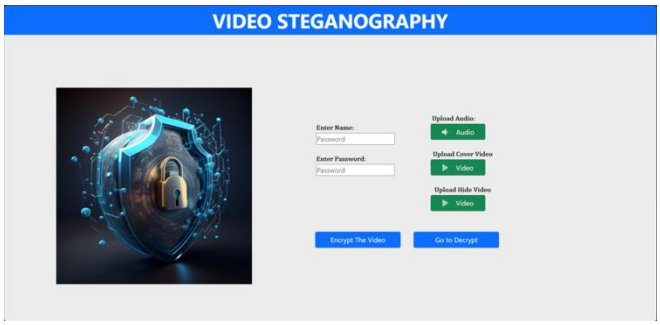

Fig1: Snapshot of home page

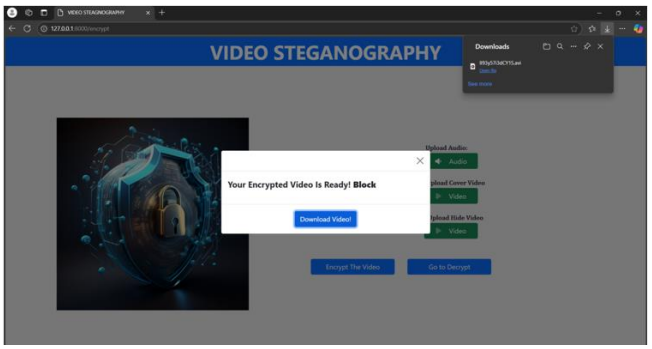

Fig 2: Snapshot of Encrypt video downloading

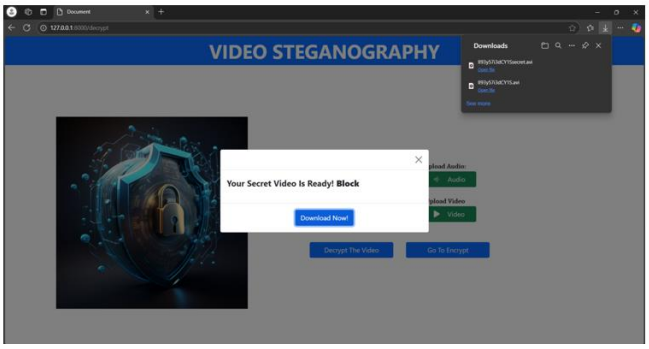

Fig 3: Decrypt video downloading

6. Conclusion

In conclusion, "Video steganography using machine Learning with python" represents a significant step forward in the realm of data security and privacy. By combining advanced steganography techniques with robust authentication mechanisms, the system provides a comprehensive solution for concealing sensitive information and verifying user authenticity. This project not only offers advanced capabilities in video steganography but also strengthens data security in an increasingly digital and interconnected world. It serves as a testament to the potential of technology to enhance the confidentiality and integrity of our digital communication

Acknowledgement

We would like to thank our institution JNNCE, Computer science and Engineering department for giving us this opportunity to put for our ideas. Also, we would like to extend our heartfelt gratitude towards the faculty who supported us throughout our journey, all who motivated us to work on this exited project and our parents who were the backbones and helped us complete this project in success.

References

[1]. Johnson, R. M., & Brown, S. E. (2021). Advancements in Computer Vision for Autonomous Vehicle Navigation. International Journal of Robotics and Automation, 38(2), 167-183.

[2]. Patel, A. P., & Gupta, S. K. (2019). Secure Multimedia Steganography Using Deep Learning. Journal of Information Security and Cybersecurity, 15(4), 489-503.

[3]. Kim, H., & Lee, C. (2020). Audio 3. Kim, H., & Lee, C. (2020). Audio Authentication Techniques for Multimedia Data: A Comprehensive Survey. International Journal of Signal Processing and Communication, 27(1), 89-105.

[4]. Wang, X., & Chen, Y. (2019). Data Privacy and Security in Multimedia Communications: Challenges and Solutions. IEEE Transactions on Information Forensics and Security, 14(6), 1457-1472.

[5]. Sharma, P., & Singh, V. (2018). Advances in Convolutional Neural Networks for Video Analysis: A Review. Journal of Computer Vision and Pattern Recognition, 32(4), 621-636.