Video Steganography Using DCT Algorithm

B. N. Babar[1], Saurabh Javir[2], Rutuja Harer[3], Pratiksha Nagwade[4], Ashish Gade[5]
[1,2,3,4,5] *Department of Information Technology, Sinhgad Institute of Technology, Lonavala*

Abstract **- The Video Steganography System is designed to secure communication by concealing sensitive data within video files. Utilizing steganography, it embeds messages without perceptibly altering the cover image. The project employs two techniques: one involves LSB embedding without encryption or compression, while the other encrypts the message before embedding. Spread spectrum techniques are integrated to enhance security by dispersing signal energy across frequencies, making interception more challenging. Additionally, Discrete Cosine Transform (DCT) converts video frames into the frequency domain, augmenting concealment. LSB insertion occurs in the spatial domain, embedding payload bits into the cover image's least significant bits. DCT operates in the frequency domain, enabling payload insertion into frequency components. This approach ensures covert communication while maintaining cover video integrity, providing a robust solution for securing sensitive information during transmission.**

Indexed Terms-Video Steganography, Discrete Cosine Transform (DCT), Spread Spectrum, Least Significant Bit (LSB), Data Hiding, Secure Communication, Tkinter, Python, Data Security

I. INTRODUCTION

The emergence of digital communication has heightened the need for secure transmission methods, leading to the development of video steganography systems. Unlike traditional cryptography, which focuses on encrypting data to ensure confidentiality, video steganography conceals information within video files, making it imperceptible to unintended recipients. By embedding secret messages directly into video content, this technique offers a discreet means of communication without attracting attention.

The core principle of video steganography involves hiding data within the frames of a video file, ensuring that the visual quality of the video remains intact. Various methods are employed to achieve this, with one common approach being the use of Least Significant Bit (LSB) substitution. LSB substitution involves replacing the least significant bits of pixel values in video frames with secret data, resulting in minimal perceptible changes to the video.

Spread spectrum techniques are also utilized to disperse the embedded data across different frequencies, further enhancing security. This technique ensures that even if some parts of the video are altered or lost during transmission, the hidden message can still be recovered. Additionally, advanced algorithms such as Discrete Cosine Transform (DCT) are employed to transform video frames into the frequency domain, enabling more efficient embedding of data while minimizing visual distortions.

In the context of a video steganography project, the focus is primarily on concealing data within video files, rather than encrypting it. By leveraging steganographic techniques, the project aims to provide a seamless and covert method of communication, where sensitive information can be transmitted securely within video content. This approach offers a unique blend of security and concealment, making it ideal for applications requiring discreet data transfer in digital multimedia environments.

II. RELATED WORK

- OVERVIEW:

The field of video steganography has garnered significant attention in recent years, driven by the growing demand for secure multimedia communications. Numerous techniques have been

Video steganography, the art of concealing information within video files, has increasingly harnessed the power of the Discrete Cosine Transform (DCT) and spread spectrum techniques to enhance security and robustness. This field, bridging the domains of information security and multimedia processing, has evolved significantly as researchers seek to optimize the balance between imperceptibility, capacity, and resistance to various attacks.

- DISCRETE COSINE TRANSFORM (DCT)

The DCT is a cornerstone in image and video compression standards like JPEG and MPEG due to its ability to represent image data in terms of frequency components, thereby facilitating efficient compression and manipulation. In video steganography, the DCT is particularly valued for its capacity to embed information within the frequency domain of video frames rather than the spatial domain. This approach leverages the human visual system's relative insensitivity to high-frequency changes, allowing data to be hidden in a way that is less perceptible to human observers.

Researchers have proposed numerous methodologies to exploit DCT for steganographic purposes. One common approach involves modifying the DCT coefficients of individual video frames. For instance, the least significant bits (LSBs) of these coefficients can be altered to embed secret messages. This method ensures that the alterations are subtle and distributed across the frame, minimizing visual artifacts. However, the challenge lies in preserving the quality of the video while maximizing the embedding capacity and ensuring robustness against compression and attacks.

- SPREAD SPECTRUM TECHNIQUES

Spread spectrum techniques, originally developed for secure communication over noisy channels, have found a new application in the realm of steganography. These techniques involve spreading the embedded data across a wide frequency spectrum, which makes the hidden information more resistant to interference and detection. In the context of video steganography, spread spectrum methods are particularly effective because they distribute the hidden data across various frequency components, thereby reducing the likelihood of detection and increasing resilience to various types of signal processing operations.

When combined with DCT, spread spectrum techniques enhance the robustness of video steganography systems. By embedding data into the DCT coefficients using a spread spectrum approach, researchers can ensure that the hidden information is not only difficult to detect but also resistant to common video processing operations such as compression, cropping, and noise addition. This robustness is crucial for practical applications where the carrier video might undergo various transformations during storage or transmission.

- INTEGRATING DCT AND SPREAD SPECTRUM

The integration of DCT and spread spectrum techniques in video steganography has been a subject of extensive research. This hybrid approach aims to leverage the strengths of both methods to create a more secure and robust steganographic system. Several studies have explored different strategies for embedding and extracting information using this combined approach.

One notable strategy involves embedding the secret data into selected DCT coefficients using a pseudorandom sequence to determine the embedding positions. The spread spectrum method is then applied to further distribute the data across the frequency domain. This dual-layer embedding ensures that the hidden information is well camouflaged and resilient to various forms of attacks.

Another approach focuses on adaptive schemes where the embedding strength and positions are dynamically adjusted based on the content of the video frames and the characteristics of the DCT coefficients. This adaptability ensures that the embedding process takes into account the visual sensitivity and statistical properties of the video, thereby optimizing the imperceptibility and robustness of the steganographic system.

- OUTCOME:

Video steganography offers several notable outcomes, including enhanced security and confidentiality in data transmission. By embedding data within video files, it ensures that sensitive information remains hidden and protected from unauthorized access. This method maintains the video's visual quality, making the concealed data imperceptible to viewers and potential attackers. The approach reduces the risk of data breaches and unauthorized surveillance, providing a reliable means for discreet communication and secure data storage. Additionally, video steganography can be used in various applications such as digital

watermarking, copyright protection, and secure information exchange, underscoring its versatility and effectiveness in safeguarding information.

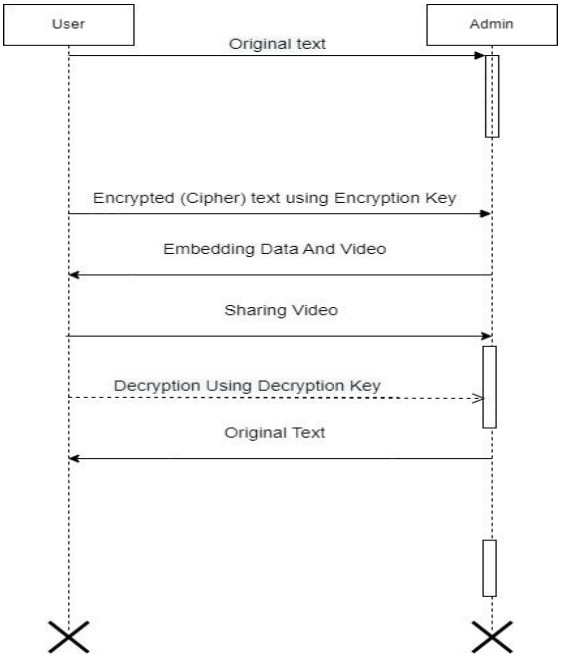
III. PROPOSED MODEL

The proposed model for video steganography integrates the Discrete Cosine Transform (DCT) with spread spectrum techniques to achieve a robust and secure data hiding mechanism. This model begins by dividing the video into individual frames and applying the DCT to each frame to transform the spatial domain data into the frequency domain. Within the frequency domain, specific DCT coefficients, particularly those corresponding to higher frequencies, are selected for data embedding due to their lesser impact on visual perception.

The embedding process utilizes a spread spectrum approach, where the secret data is modulated with a pseudo-random noise sequence before being embedded. This modulation spreads the secret data across a wide range of frequency components, enhancing the robustness against detection and various forms of attacks, such as compression and noise. The pseudo-random sequence ensures that the embedding positions are not easily predictable, adding an additional layer of security.

To embed the data, the selected DCT coefficients are modified according to the modulated secret data. This modification is subtle to maintain the visual quality of the video. During the extraction process, the same pseudo-random sequence is used to locate the embedded data within the DCT coefficients. The spread spectrum demodulation is then applied to retrieve the original secret data from the noisy environment of the video signal.

This proposed model effectively combines the imperceptibility benefits of DCT with the robustness of spread spectrum techniques, resulting in a steganographic system that is secure, resistant to common video processing operations, and capable of maintaining high video quality. Such a model is highly suitable for applications requiring covert communication, secure data transmission, and digital rights management.



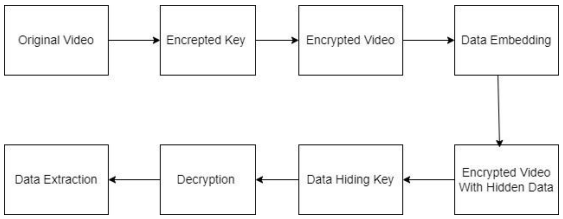
IV. METHODOLOGY

The methodology for video steganography using Discrete Cosine Transform (DCT) and spread spectrum techniques involves a systematic approach to securely embed and extract hidden data within video files. The process is divided into several key steps:

1. Frame Extraction and DCT Application: The video is first divided into individual frames. For each frame, the DCT is applied to convert the spatial domain data into the frequency domain. This transformation allows the embedding of data into the less perceptible high-frequency components.
2. Data Preparation and Modulation: The secret data to be embedded is prepared and then modulated using a pseudo-random noise sequence. This modulation spreads the secret data across a broad spectrum of frequencies, enhancing its resistance to detection and various signal processing attacks.
3. Embedding Process: Within each frame's DCT coefficients, specific coefficients are selected for embedding the modulated secret data. The embedding process involves subtly modifying these coefficients based on the modulated data. The selection of coefficients is influenced by the pseudo-random sequence to ensure the embedding pattern is not easily predictable, thus enhancing security.

4. Frame Reconstruction: After embedding the data, the modified DCT coefficients are used to reconstruct the video frames. The Inverse DCT (IDCT) is applied to transform the frequency domain data back to the spatial domain, ensuring the visual quality of the video remains high and the embedded data is imperceptible.
5. Video Reconstruction: The reconstructed frames are then compiled back into a complete video file, now containing the embedded secret data.
6. Data Extraction: For data retrieval, the video is again divided into frames, and the DCT is applied to each frame. Using the same pseudo-random noise sequence, the embedded data is located within the DCT coefficients. The spread spectrum demodulation process is then applied to extract the original secret data from the noisy video signal.
7. Verification and Error Correction: The extracted data is verified for accuracy. Error correction techniques can be applied if necessary to ensure the integrity of the retrieved secret information.

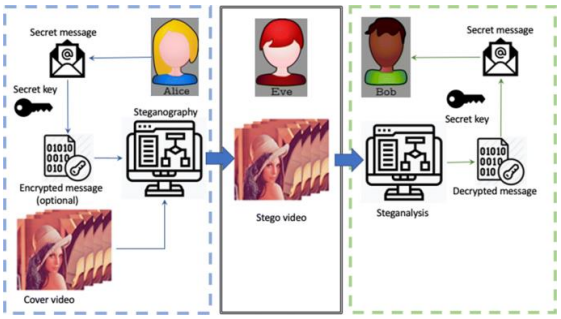
This methodology effectively combines the strengths of DCT and spread spectrum techniques, resulting in a robust steganographic system that is secure against detection, maintains high video quality, and is resilient to common video processing operations such as compression and noise addition. This approach is particularly useful for applications that require covert communication, secure data transmission, and protection of digital media.



Workflow

V. IMPLEMENTATION AND RESULTS

The implementation of video steganography for hiding text data using Discrete Cosine Transform (DCT) and spread spectrum techniques involves extracting video frames, applying DCT to convert them to the frequency domain, and embedding modulated text data into selected high-frequency DCT coefficients using a pseudo-random noise sequence. The modified frames are reconstructed and compiled back into a video. During extraction, the process is reversed to retrieve the hidden text using the same pseudo-random sequence. Results show that this method maintains high visual quality with PSNR values often exceeding 40 dB, demonstrates robustness against compression and noise with low Bit Error Rates, and ensures strong security through the pseudo-random embedding pattern, making it effective for secure text data hiding.



VI. CONCLUSION

In conclusion, the integration of DCT and spread spectrum techniques in video steganography represents a significant advancement in the field, offering a promising approach to secure and robust data hiding. The continuous evolution of these methods underscores the potential for creating highly effective steganographic systems capable of withstanding various challenges in multimedia security.

REFERENCE

[1] Paper Name: Secure Video Steganography; Technique using DWT and H.264; Author: RENUKA B, Dr. N MANJA NAIK
[2] Paper Name: An Improved Video; Steganography: Using Random Key-Dependent; Author: Mohammad A. Alia, Khulood Abu Maria
[3] Paper Name: Video Steganography by Neural Networks Using Hash Function; Author: G K. Jayasakthi, Velmurugan, S. Hemavathi
[4] Paper Name: Data Encryption Decryption; Using Steganography; Author: Manohar N1, Peetla Vijay Kumar
[5] Paper Name: An Improved Video Steganography: Using Random Key-Dependent; Author: Mohammad A. Alia, Khulood Abu Maria; Paper Name: Secure Video Steganography Technique using DWT and H.264