JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Video-Steganography with Fake DNA and complex Frames.

Mrs. Amrita Arjun Kindalkar, Ms. Nisarga, Ms.Pavitra, Ms. Pooja D, Ms. Sangeeta

Department of Computer science and Engineering

Srinivas University

Institute of Engineering and Technology, Mukka Mangalore, India

Abstract-- This paper presents a secure method for hiding data within video files using a combination of Blowfish encryption and video steganography. First, the sensitive information is encrypted using Blowfish, a robust encryption algorithm, and then embedded into the video frames by converting the encrypted data into a fake DNA sequence, which is hidden in the least significant bits of the video, ensuring minimal visual distortion. The system extracts the hidden data by analyzing the video frames, identifying changes, and reversing the encoding process to recover the original message, which is then decrypted using Blowfish. This approach enhances security by combining both encryption and steganography, offering a reliable solution for secure communication while maintaining the quality of the video .

***Keyword*: Video,Blowfish,DNA and Complex frame.**

I. INTRODUCTION

In today's digital age, keeping sensitive information secure during transmission is essential. While traditional encryption methods can protect data, they can still be vulnerable to being detected or intercepted. To address this, steganography—hiding data within other types of media like videos—adds an extra layer of security. This paper introduces a method that combines encryption and steganography to safely embed data into video files, making it hard for unauthorized individuals to detect or access the information.

The system uses Blowfish, a strong and efficient encryption algorithm, to encrypt messages before they are hidden in video files. Blowfish is a popular choice because it offers strong protection with fast performance. The encrypted data is then encoded into a fake DNA sequence and embedded into the least significant bits of the video, which allows the data to be hidden without affecting the visual quality of the video. To make sure the data is hidden effectively, the system analyzes the video frames and identifies the best spots where the data can be embedded without noticeable changes. This is done by selecting frames with more complex changes, using a method called Discrete Cosine Transform (DCT). Once these frames are found, the data is hidden in them, and the video is put together for sending.

On the receiving end, the system extracts the hidden data by analyzing the video frames and reversing the encoding process. After the data is recovered, it's decrypted using Blowfish to reveal the original message. By combining encryption with steganography, this approach provides a secure way to communicate confidentially through video, without compromising the quality of the video itself.

II. RELATED WORK

In recent years, securing data during transmission has become increasingly important, especially with the rise in cyber threats and privacy concerns. Various methods have been proposed to ensure the confidentiality of sensitive information, and two primary techniques—encryption and steganography—have gained significant attention. These techniques, both individually and in combination, have been

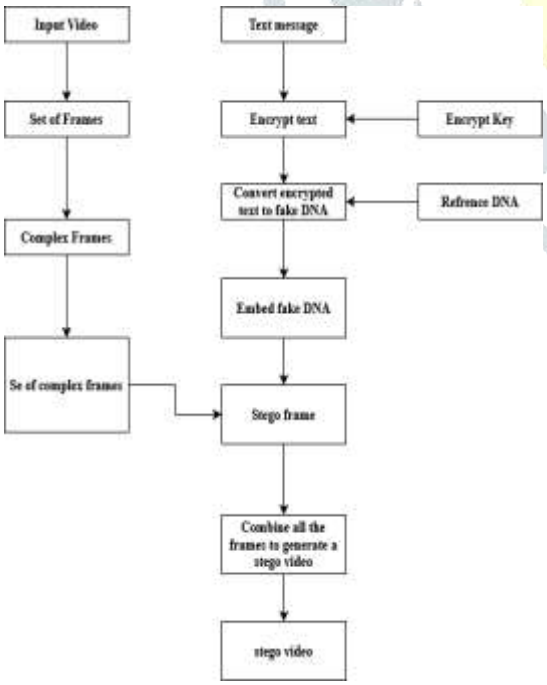
explored for their ability to protect and conceal data. This section reviews existing research on encryption, steganography, and their integration in secure communication systems, with a focus on video- based steganography.

1. Encryption Techniques

Encryption algorithms, such as AES, RSA, and Blowfish, have been widely used to protect sensitive data. These algorithms secure data by transforming it into unreadable ciphertext, ensuring that even if intercepted, the data remains inaccessible without the decryption key. Blowfish, in particular, is known for its efficiency and strong security features, making it an ideal choice for securing messages in our proposed system. Despite its strengths, traditional encryption alone can sometimes draw attention to sensitive data during transmission, leading to potential risks.

2. Steganography Approaches

Steganography is the practice of hiding secret information within innocent-looking files, such as



images, audio, or videos. By embedding data in these files, steganography ensures that the presence of sensitive information remains undetectable. The most common technique used in steganography is hiding data in the least significant bits (LSBs) of media files, which minimally alters the visual or audio quality. Research has shown that hiding information in images or videos allows for discreet communication, reducing the likelihood of detection by unauthorized parties highly coherent facial expressions over extended durations.

3. Combining Encryption and Steganography

To strengthen data security, several studies have explored the combination of encryption and steganography. The idea is to first encrypt data using a strong encryption algorithm like Blowfish, and then embed the encrypted data within a media file using steganography. This layered approach ensures that even if the hidden data is detected, it remains unintelligible without decryption. Researchers have successfully used this method in image and audio files, where the encrypted data is embedded in pixel values or audio samples.

4. Video Steganography Advancements

While image steganography is well-established, video steganography has gained more attention due to the larger capacity for storing data. Video files offer both spatial and temporal dimensions, allowing for more sophisticated methods of embedding data. Recent studies have focused on embedding data in specific frames based on motion analysis or content complexity. By selecting frames that exhibit more subtle changes, these methods ensure that the hidden data has minimal impact on video quality, making the steganography process harder to detect.

5. Discrete Cosine Transform (DCT) in Video Steganography.

Discrete Cosine Transform (DCT) has been employed in video steganography to identify complex regions of the video where data can be securely hidden. DCT is a mathematical transform used in image and video compression, which helps analyze the frequency components of the video frames. By embedding data in high-frequency regions, researchers ensure that the data is less noticeable to viewers and does not interfere with the primary content of the video. This method has been successfully used to balance

the trade-off between embedding efficiency and video quality.

III. SYSTEM DESIGN

1. **Introduction to the proposed system:**The proposed system utilizes a novel approach to video steganography by embedding encrypted text within complex frames using a fake DNA sequence. Traditional steganographic techniques often embed data in image pixels or audio signals, which can be susceptible to detection and attacks. However, this method leverages the complexity of video frames and DNA-based encoding to enhance security.

The process begins with an input video, which is divided into a sequence of frames. From these frames, a subset of complex frames is selected based on specific criteria, ensuring robustness and resistance to visual

distortions or steganalysis attacks.

2. **Encryption and Fake DNA Generation:**To further strengthen security, the secret message intended for embedding undergoes an encryption process using a secure encryption key. This ensures that even if the hidden data is extracted, it remains unintelligible without the proper decryption key. Once encrypted, the message is converted into a fake DNA sequence by referencing a predefined DNA structure. DNA-based encryption is inspired by biological principles and adds an additional layer of complexity, making it difficult for attackers to interpret the encoded data. This step significantly enhances the confidentiality and uniqueness of the embedded information.

3. Embedding Process and Stego Frame Formation: After generating the fake DNA sequence, it is embedded into the selected complex frames. These frames are chosen strategically to minimize perceptual differences, ensuring that the hidden information does not alter the visual quality of the video. The embedding process modifies specific pixel values or other frame properties in a way that remains undetectable to human vision and common steganalysis techniques. Once embedding is completed, the modified frames are referred to as stego frames. These stego frames now contain the hidden data while maintaining their original structure, making them indistinguishable from the unmodified frames. 4.**Stego Video Reconstruction and Security Benefits:**In the final stage, all the stego frames are recombined to reconstruct the stego video. This video appears identical to the original but securely conceals the encrypted message within selected frames. The use of complex frames.

IV. IMPLEMENTATION

Implementing video steganography using DNA encoding and complex frames involves a systematic process to discreetly hide data within a video. First, the data is encoded into DNA sequences, converting binary information into nucleotide bases. Complex frames, which are characterized by rapid motion or intricate patterns, are selected as ideal spots for embedding the DNA to reduce visual disruption. During extraction, the embedded DNA is detected from these complex frames, decoded back into binary data, and the hidden message is retrieved. The system is tested for imperceptibility, capacity, and resistance to attacks to ensure optimal performance. Ethical considerations are integral, ensuring compliance with legal standards, while continuous research improves the technique's effectiveness and ability to evade detection.

The Frame Selection Algorithm is designed to identify complex frames in a video sequence. It starts by preprocessing the input video, treating it as a sequence of frames, and defining complex frames as those that significantly differ from the previous frame. To analyze these differences, the algorithm applies the Discrete Cosine Transform (DCT) on each frame, converting spatial information into frequency data. It then calculates the mean value of the DCT coefficients for each frame, which helps measure the energy distribution or content in the frequency domain. By comparing the mean values of consecutive frames' DCT coefficients, the algorithm identifies frames with notable changes in frequency content. These frames are stored in an array for further processing. Finally, the output is an array containing the selected complex frames.

The Data Encryption Algorithm is used to convert cipher text into a fake DNA sequence for steganographic purposes. Initially, the cipher text is converted into its binary representation. The DNA complementary rule is then applied to each binary pair, modifying the original binary sequence. The modified binary sequence is iterated, and specific operations are performed on each pair. Finally, the modified binary pairs are used to generate the fake DNA sequence, which is then ready for embedding into the video.

VI. RESULTS AND ANALYSIS

Video Steganography using DNA and Complex Frames is a technique that hides secret data inside a video by turning it into DNA sequences (using the letters A, C, G, T) and embedding them in frames with fast motion or complex patterns. These specific frames are chosen because they help conceal the hidden data without affecting the video’s appearance. When it's time to retrieve the hidden information, the DNA sequences are extracted from the frames, converted back into binary, and then decoded to reveal

the original

secret message. This method provides a secure and discreet way to hide data within a video..

VII. CONCLUSION

In conclusion, Video Steganography using DNA and Complex Frames provides a powerful and secure technique for hiding secret information within video files. By encoding data into DNA sequences and embedding these sequences in complex frames, the method effectively conceals sensitive information without compromising the video's appearance. The use of DNA sequences adds a layer of complexity, while complex video frames, characterized by rapid motion or intricate patterns, serve as ideal locations to hide the data. This ensures the hidden information remains undetected and protected from unauthorized access.

This approach not only enhances security but also offers a high degree of flexibility. It allows for the embedding of significant amounts of data within videos, making it an ideal solution for scenarios where secure communication and data protection are paramount. Whether used in securing personal information, confidential communications, or intellectual property, the technique offers a discreet and reliable means of safeguarding sensitive content.

The potential applications of this method extend to various fields, including secure communication, cybersecurity, and digital forensics. As digital security threats continue to evolve, the need for innovative methods like Video Steganography using DNA and Complex Frames becomes even more critical. By providing an advanced way to protect and conceal data, this technique represents a valuable contribution to the ongoing efforts in enhancing information security and privacy in an increasingly digital world.

REFERENCES

1. Dr. Manjula G R, Raksha P K, Shraddha C S Atreya, Swathi H R, Vaishnavi N (2024) . Video Steganography with DNA and complex frames.

2. Asma Sajjad, Humaira Ashraf. "Improved Video Steganography with Dual Cover Medium, DNA and Complex Frames", 31 October 2022.

3. Shaohua Wan, Xiaolong Xu. "An Intelligent Video Analysis Method for Abnormal Event Detection in Intelligent Transportation Systems", IEEE Transactions on Intelligent Transportation Systems, July 2021.

4. N. Kar, K. Mandal and B. Bhattacharya, "Improved chaosbased video steganography using DNA alphabets," ICT Express, vol. 4, pp. 6–13, 2018.

5. Partha Saha, Lubna Yasmin Pinky, Mohammad Ashraful Islam, Papia Akter, "Higher Payload Capacity in DNA Steganography using Balanced Tree Data Structure", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878 (Online), Volume-8 Issue-4, November 2019.

6. Z.L.Yi and Z.W.Dong, "A novel steganography algorithm based on motion vector and matrix encoding," in Proc. IEEE 3rd Int. Conf. on Communication Software and Networks, Xian, China, pp. 406–409, 2011.

7. S.Mumthas and A.Lijiya, "Transform domain video steganography using RSA, random DNA encryption and huffman encoding", in Proc. Computer Science, Cochin, India, vol. 115, pp. 660–666, 2017.

8. Marghny H. Mohammed and Alaa Abdel- Razeq, "DNAbased steganography using genetic algorithm", Information Science Letters, 1 Sept. 2020.

9. Malathi Pa, Manoaj Ma, "Highly Improved DNA Based Steganography", 7th International Conference on Advances in Computing & Communications, ICACC-2017, 22- 24

10. Gat Pooja Rajkumar, Virendra S Malemath, "Video Steganography: Secure Data HidingTechnique", I. J. Computer Network and Information Security, Sept 2017