IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, November 2023

Video and Image Steganography

Prof. B. N. Babar[1], Saurabh Javir[2], Pratiksha Nagawade[3], Ashish Gade[4], Rutuja Harer[5]
Assistant Professor, Department of Information Technology[1]
Students, Department of Information Technology[2,3,4,5]
Sinhgad Institute of Technology, Lonavala, Maharashtra, India

Abstract: *Video steganography, a technique for embedding secret information within video sequences, has gained prominence in the domain of covert communication. By exploiting the inherent redundancy and high capacity of video data, this approach enables secure data transmission without raising suspicion. This paper delves into the intricacies of AES-based video steganography, with a particular focus on the integration of the Advanced Encryption Standard (AES) algorithm. The AES algorithm, renowned for its robust encryption capabilities, serves as a cornerstone of this steganographic approach. By encrypting the secret data prior to embedding it within the video frames, an additional layer of security is introduced, safeguarding the confidentiality of the hidden information.*

Keywords: Video Steganography, Encryption, Decryption, AES, Hidding data

I. INTRODUCTION

Video steganography is a technique for hiding secret information within video sequences. AESor Advanced Encryption Standard, is a widely used symmetric-key block cipher algorithm that has gained prominence in video steganography due to its robust encryption capabilities. The integration of AES into video steganography offers several distinct advantages, including enhanced security, resilience against attacks, and compatibility with existing steganographic techniques. However, the use of AES also introduces some challenges, such as reduced embedding capacity and computational overhead. Despite these challenges, AES-based video steganography remains a valuable tool for secure data hiding in video sequences.

II. MOTIVATION

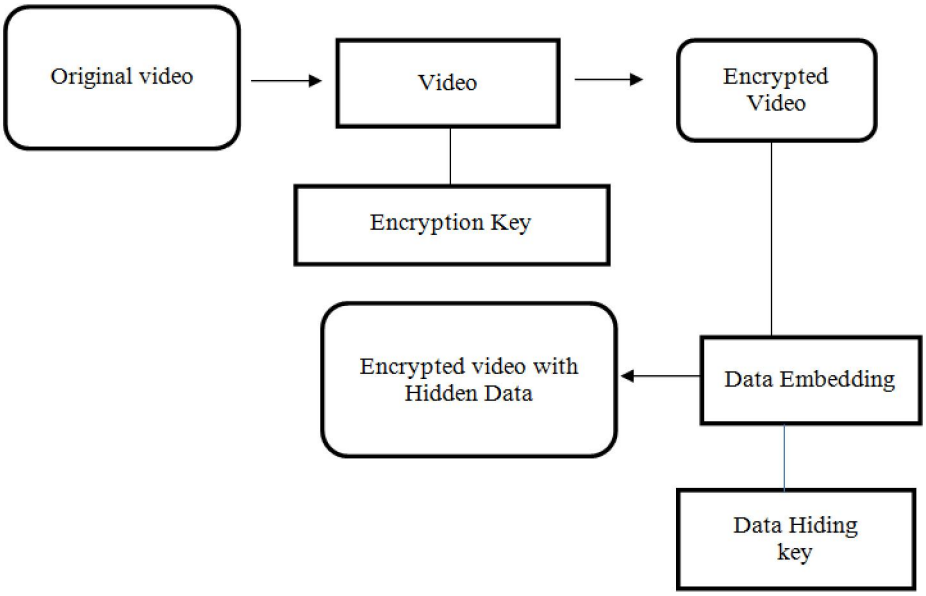
"Steganography conceals information to avoid suspicion, employing techniques to hide data in various carriers like audio, images, text, and videos. The assignment focuses on the advantages of Image Steganography. Firstly, our scheme's embedding capacity is proportional to stego texture image size due to texture synthesis. Secondly, the steganographic approach is resistant to steganalytic algorithms as the stego texture is formed from a source texture, not by modifying existing image contents. Thirdly, our scheme's reversible capability allows recovery of the exact source texture, enabling the continuation of secret messages in subsequent rounds if necessary."

III. OBJECTIVE

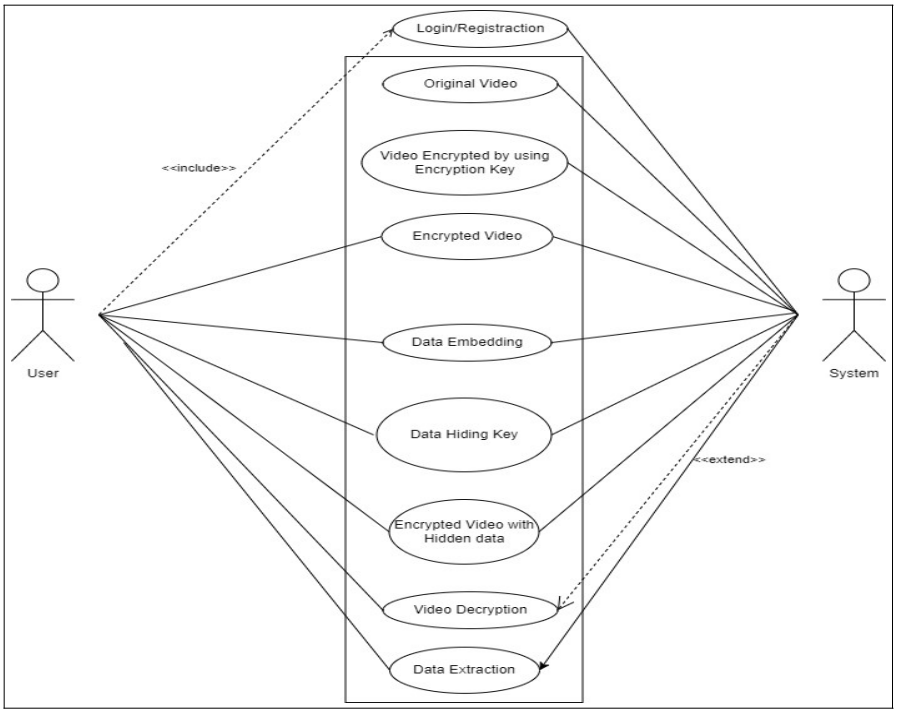
The objective of this project is to investigate and evaluate the performance of AES-based video steganography using various embedding techniques. The performance will be evaluated in terms of embedding capacity, imperceptibility, and robustness against attacks. The project aims to identify the most effective and efficient approach for secure data hiding in video sequences, while also exploring adaptive embedding strategies and investigating the use of additional security measures

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, November 2023

IV. SYSTEM ARCHITECTURE



UML Diagram:



Data Flow Diagrams:

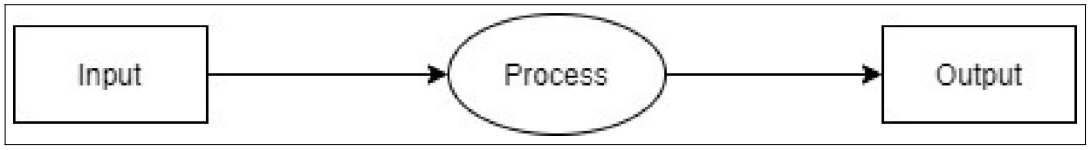


Figure: Data Flow diagram 0 level

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, November 2023

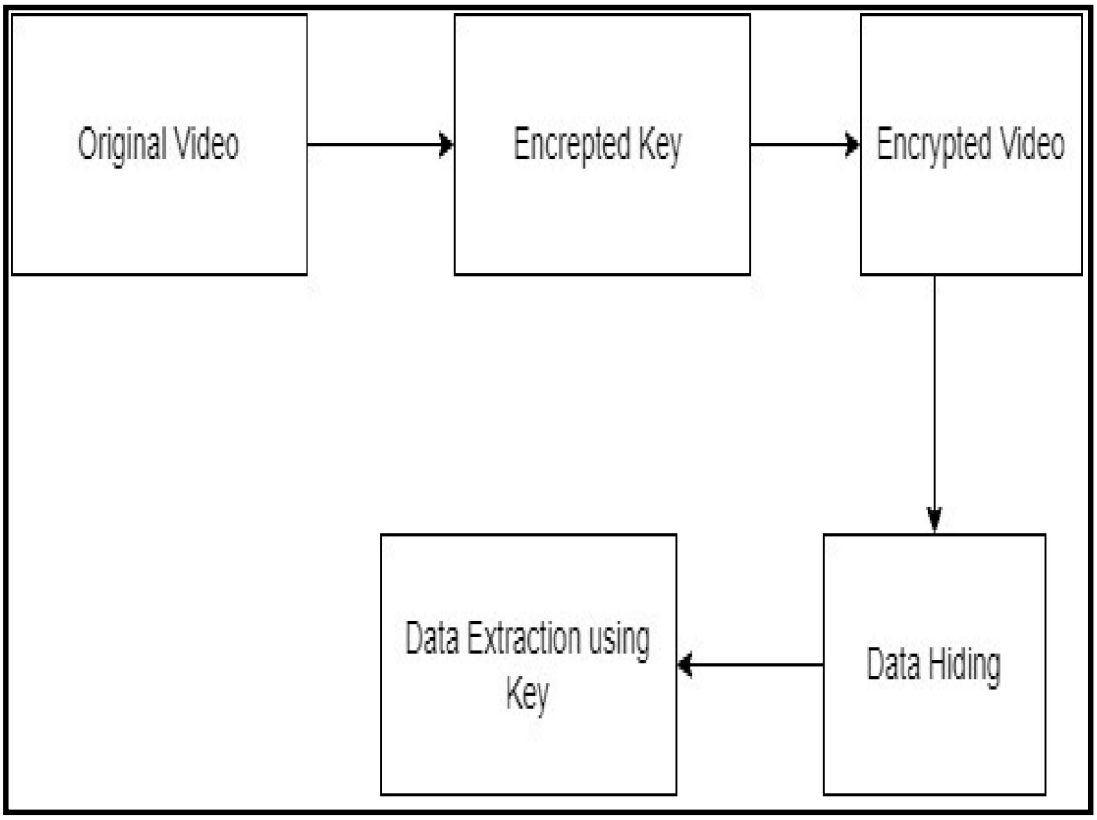


Figure: Data Flow diagram 1 level

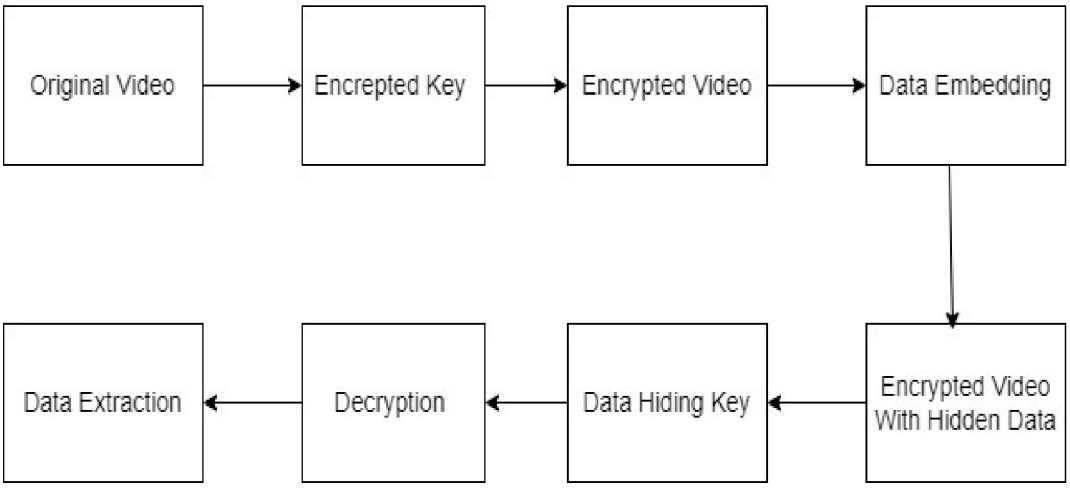


Figure: Data Flow diagram 2 level

V. SOFTWARE REQUIREMENTS

- System : Intel I5 Processor.
- Hard Disk : 40 GB.
- Monitor : 15. 8 GB
- Ram : 8GB

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 2, November 2023

VI. HARDWARE REQUIREMENTS

- Operating system : Windows 10.
- Coding Language : Python
- IDE : Spyder
- Database : SQLite.

VII. APPLICATIONS

1. Forensic Analysis

Digital Forensics: Law enforcement agencies use video steganography to analyze videos for hidden information related to criminal activities, providing crucial evidence in investigations

2. Medical Imagery:

Patient Data Protection: Steganography can be applied to medical imagery and videos to embed patient information securely, ensuring privacy and compliance with healthcare regulations.

VIII. CONCLUSION

This paper proposes new ways to hide information in images and videos. One of the methods, called deep steganography, uses a computer program to learn how to hide information in images in a way that is difficult to detect. The paper also proposes ways to make it more difficult for attackers to recover the hidden information.

IX. ACKNOWLEDGMENT

"We are delighted to present the preliminary project report on the topic 'Video Steganography.' We extend our gratitude to our internal guide, Prof B.N Babar Sir, for providing us with the necessary help and guidance. We appreciate his kind support, and his valuable suggestions have been instrumental in the development of our project."

REFERENCES

[1]. Bhargava, S., Mukhija, M. (2019). HIDE IMAGE AND TEXT USING LSB, DWT AND RSA BASED ON IMAGE ST EGANOGRAPHY. ICTACT Journal on Image Video Processing, 9(3)

[2]. Srilakshmi, P., Himabindu, C., Chait anya, N., Muralidhar, S. V.,Sumanth, M. V., Vinay, K. (2018). TEXT EMBEDDING USING IMAGE ST EGANOGRAPHY IN SPATIAL DOMAIN. International Journal of Engineering Technology, 7(3.6), 14.

[3]. Krishnaveni, N. (2018). IMAGE STEGANOGRAPHY USING LSB EMBED- DING WIT H CHAOS. International Journal of Pure and Applied Mathematics, 118(8), 505-509.

[4]. Karanjit Kaur Baldip Kaur (2018). "DWT-LSB Approach for Video Steganography using Artificial Neural Network". In International Advanced Research Journal in Science, Engineering and Technology, IARJSET.

[5]. Mehdi Boroumand, Mo Chen Jessica Fridich (2018). "Deep Residual Network for Steganalysis of Digital Images". 2018 IEEE.

[6].M. Dalal and M. Juneja, "A robust and imperceptible steganography technique for SD and HD videos," Multimed Tools Appl, vol. 78, no. 5, pp. 5769–5789, Mar. 2019, doi: 10.1007/s11042-018-6093-3

[7].1016/j.image.2018.03.012