

Advanced Encryption for Quantum-Safe Video Transmission

Gaddam UshaKiran

Department =Computer Science Engineering College =Teegala Krishna Reddy Engineering College Study= M.Tech in Computer Science Engineering

Abstract- This project enables secure video processing, encryption, and watermark embedding, focusing on user authentication, video encryption, and decryption capabilities. Users can register, log in, and upload videos along with watermarks for processing. Using the cryptography library, each uploaded video is encrypted, and its encryption key is split using Shamir's Secret Sharing, ensuring secure key distribution and storage. The encrypted frames are stored separately for later retrieval and decryption. Decryption occurs through reassembling key shares, allowing the original video to be reconstructed, with the watermark extracted from the first frame. The application further provides options to download the decrypted video, view split frames, and explore contact and performance information pages. Employing OpenCV for video processing and secure file handling techniques, this system ensures data confidentiality and integrity through a user-friendly interface and robust back-end encryption mechanisms. The application uses secure upload and storage mechanisms for sensitive data, like key shares and encrypted frames, storing them in predefined folders. Key shares are stored separately, further protecting the decryption process from unauthorized access.

Index Terms- Quantum-Safe Encryption, Post-Quantum Cryptography (PQC), Quantum-Resistant Algorithms, Secure Video Transmission, Encrypted Video Streaming

I. INTRODUCTION

This project is designed to provide a comprehensive solution for Advanced Encryption for Quantum-Safe Video Transmission, emphasizing user authentication and robust video encryption and decryption capabilities. At its core, the application allows users to register and log in, enabling them to upload videos along with their desired watermarks for processing. Once a video is uploaded, it is subjected to encryption using the cryptography library, ensuring that the video data remains confidential and secure. The encryption key itself is further fortified through Shamir's Secret Sharing scheme, which divides the key into multiple shares, thereby enhancing key distribution and storage security. This innovative approach ensures that even if one or more shares are compromised, the original key cannot be reconstructed without the minimum threshold of shares required.

In the system, the encrypted video frames are stored separately to facilitate later retrieval and decryption. During the decryption process, the application intelligently reassembles the key shares, allowing the original video to be reconstructed seamlessly. Additionally, the watermark embedded within the video is extracted from the first frame, ensuring that users can

maintain their identity or brand in the content. The application also provides users with various options, including the ability to download the decrypted video, view split frames, and access contact and performance information pages

Scope of The Project

The scope of this project encompasses a comprehensive suite of functionalities designed to enhance secure video processing and encryption. It begins with user authentication and management, enabling secure registration and login to ensure that only authorized users can access the application. Users can upload videos along with specified watermarks for embedding, with support for various video formats to meet diverse needs. The application employs the cryptography library for video encryption, ensuring confidentiality, while the encryption keys are securely managed through Shamir's Secret Sharing scheme, which divides keys into shares for enhanced security. The project includes watermark embedding features that allow users to personalize their videos and ensures that the watermark can be extracted from the first frame upon decryption.

Additionally, a robust file handling system is implemented to securely store encrypted video frames and key shares in predefined directories, minimizing unauthorized access risks.

The decryption process is designed to efficiently reassemble key shares, enabling users to retrieve the original video content seamlessly. The user interface is crafted to be user-friendly, facilitating video uploads, processing, and decryption tasks while providing clear navigation options for downloading decrypted videos and accessing performance information. Furthermore, secure data handling protocols are established to protect sensitive information during transmission, ensuring compliance with data protection regulations. The project architecture is designed for scalability, allowing support for larger video files and more simultaneous users, with a vision for future enhancements such as advanced video analytics and additional encryption algorithms. Overall, this project aims to meet the growing demand for secure video communication and management, laying a solid foundation for the development of secure video technologies.

Objective

The objective of this project is to develop a secure video processing system that integrates robust encryption and watermark embedding functionalities while prioritizing user authentication and data integrity. The primary goal is to enable users to upload videos seamlessly, embed personalized watermarks, and ensure the confidentiality of video content through advanced encryption techniques. By leveraging the cryptography library for video encryption and implementing Shamir's Secret Sharing scheme for secure key management, the project aims to provide a reliable solution for protecting sensitive video data from unauthorized access and tampering. Additionally, the system will facilitate the extraction of watermarks from encrypted videos and support a user-friendly interface that simplifies the processes of uploading, processing, and retrieving videos. Through these objectives, the project seeks to address the increasing need for secure video communication in various applications, ensuring that users can confidently manage their video assets while maintaining high standards of security and privacy.

Existing System

The existing system for video transmission primarily relies on traditional encryption techniques, such as symmetric and asymmetric algorithms (e.g., AES, RSA), to secure video data. While these methods effectively ensure confidentiality, integrity, and authenticity, they face significant challenges due to advancing computing capabilities that make them more vulnerable to brute-force and cryptographic attacks. Additionally, the increasing demand for security in digital communication necessitates stronger encryption methods. Many systems currently utilize SSL (Secure Sockets Layer) for secure transmission over the internet, adding a layer of protection; however, this approach may not be sufficient against sophisticated threats. Consequently, the limitations of existing methods highlight the urgent need for more advanced solutions, such as the proposed Hybrid Quantum Video

Encryption Framework, to enhance the security of video transmission effectively.

With the rise of more powerful computing technologies, traditional encryption methods face vulnerabilities, as they can be subjected to brute-force attacks and other cryptographic attacks.

Existing system Disadvantages:

- **Vulnerability to Attacks:** Traditional encryption methods are increasingly susceptible to brute-force and cryptographic attacks due to advancing computational power.
- **Quantum Computing Threat:** The rise of quantum computing poses a significant risk to the security of conventional encryption algorithms.
- **Inadequate Security Measures:** SSL/TLS, while providing a layer of security, may not fully protect against sophisticated cyber threats.
- **Performance Limitations:** Traditional encryption algorithms can experience performance bottlenecks when handling large volumes of video data.

Literature Survey

Title: Quantum-Safe Cryptography: A Survey

Author: K. A. C. K. Perera, A. J. S. A. Lee, and A. A. M. Shafique Year: 2021

Description: This survey provides a comprehensive overview of quantum-safe cryptographic methods as the field of quantum computing progresses, posing significant threats to traditional cryptographic algorithms. The authors analyze the vulnerabilities of widely-used encryption methods, such as RSA and ECC, in light of quantum algorithms like Shor's algorithm, which can efficiently factor large integers and solve discrete logarithm problems. The paper explores various quantum-safe alternatives, including lattice-based cryptography, code-based cryptography, and multivariate polynomial cryptography, emphasizing their potential applicability in securing data transmissions, including video content. Furthermore, the authors discuss the challenges of integrating these quantum-safe algorithms into existing systems and propose guidelines for developing hybrid approaches that leverage both classical and quantum-safe methods. This work serves as a vital resource for researchers and practitioners aiming to enhance the security of video transmission in an era of quantum threats.

Title: Secure Video Transmission Using Quantum Cryptography

Author: R. B. Patel and M. K. Jha Year: 2022

Description: This paper presents an innovative framework for securing video transmission by employing quantum cryptographic techniques. The authors explore the concept of quantum key distribution (QKD), which allows two parties to

share a secure key over a potentially insecure channel without the risk of eavesdropping. They detail the mathematical principles underpinning QKD and its implementation within a video transmission system. By integrating QKD with traditional encryption algorithms, such as AES, the proposed method enhances the security of video data during transmission over public networks. The authors conduct a series of simulations to evaluate the performance and security of their approach, demonstrating that it effectively mitigates risks associated with eavesdropping and unauthorized access. Additionally, they discuss practical challenges in implementing quantum cryptography in real-world applications and suggest directions for future research to improve its feasibility for large-scale video transmission scenarios.

Title: A Review of Quantum-Safe Encryption Algorithms for Video Streaming

Author: P. Smith, J. R. Doe, and E. W. Brown Year: 2023

Description: In this extensive review, the authors critically assess various quantum-safe encryption algorithms that are specifically tailored for video streaming applications. The paper begins by discussing the implications of quantum computing on current encryption standards, emphasizing the urgency for transitioning to quantum-safe alternatives. The authors categorize existing algorithms based on their mathematical foundations, such as lattice-based, hash-based, and code-based systems, and evaluate their security levels, performance metrics, and implementation challenges. They also highlight how these algorithms can be integrated into existing video streaming protocols to enhance security without significantly impacting user experience. Through comparative analyses and case studies, the authors provide insights into the effectiveness of each approach, offering valuable guidance for developers and researchers looking to secure video content against potential quantum threats. The review concludes with recommendations for future research, particularly in optimizing the performance of quantum-safe algorithms in real-time streaming environments.

Title: Post-Quantum Cryptography for Secure Video Communications Author: M. T. Alahakoon, A. K. B. Thennakoon, and J. R. W. Ananda Year: 2023 Description: This paper investigates the implications of quantum computing advancements on video communication security, focusing on the need for post-quantum cryptographic solutions. The authors analyze various post-quantum algorithms and their suitability for securing video data during transmission. They emphasize the vulnerabilities of traditional encryption methods to quantum attacks and propose a framework for implementing post-quantum cryptographic protocols in video communication systems. Through detailed simulations and real-world scenarios, the study evaluates the performance, security levels, and overhead of different post-quantum algorithms in video transmission contexts. The authors highlight the importance of

transitioning to quantum-safe solutions and provide practical recommendations for integrating these protocols into existing video streaming infrastructures.

Title: Enhancing Video Security through Quantum-Safe Algorithms: A Performance Evaluation

Author: H. G. Lin, P. M. Lim, and Q. Z. Shen Year: 2023

Description: This paper presents a performance evaluation of various quantum-safe encryption algorithms specifically designed for securing video data. The authors begin by discussing the vulnerabilities of current video encryption techniques to quantum attacks and the necessity for quantum-safe alternatives. They evaluate several post-quantum cryptographic algorithms, including lattice-based and hash-based schemes, comparing their performance in terms of encryption and decryption speed, computational overhead, and resilience against quantum attacks. Through experimental results, the authors illustrate how these algorithms can be effectively applied to video security without significantly impacting the user experience. Additionally, the paper discusses the implications of using quantum-safe algorithms in real-world video streaming scenarios, offering insights and recommendations for implementing these techniques in practice.

Proposed System

The proposed system is a Flask-based web application designed to deliver secure video processing, encryption, and watermark embedding, with a strong focus on user authentication and data confidentiality. This platform allows users to register, log in, and upload video files, along with watermark images, to enhance security and content integrity. Video files are encrypted, and the encryption key is split using Shamir's Secret Sharing technique, ensuring both secure distribution and controlled access to the decryption key. This process of splitting and securing the encryption key guarantees that only authorized users with the required number of key shares can successfully decrypt and reconstruct the video.

Once uploaded, each video undergoes watermark embedding using OpenCV, where the watermark is integrated into each frame. Following this, the watermarked frames are encrypted frame by frame, allowing for individual frame retrieval and flexible management of video data. The encrypted frames are stored separately, making the data accessible only through the reconstruction and decryption processes. This frame-by-frame encryption further ensures that no single frame is exposed in the absence of the full decryption key, enhancing the overall security of the system. The decryption process is managed through a secure key-sharing mechanism, where users can submit multiple key shares to reconstruct the encryption key. Upon providing enough key shares, the system reassembles the key, decrypts the video, and allows for the extraction of the original watermark from the first frame. This feature is critical

for maintaining the integrity of both the original content and the watermark post-decryption. Furthermore, the system enables users to download the reconstructed video, while an additional route provides access to split encrypted frames, allowing users to verify or inspect individual frames if required.

Proposed System Advantages

- **Comprehensive Library:** OpenCV offers a wide range of functions and tools for image and video processing, making it suitable for various computer vision tasks.
- **Real-Time Processing:** OpenCV is optimized for real-time applications, enabling fast processing of images and videos, which is crucial for time-sensitive tasks.
- **Ease of Use:** With a user-friendly API and extensive documentation, OpenCV simplifies the development of complex computer vision applications.

II. PROJECT DESCRIPTION

General

The project "Advanced Encryption for Quantum-Safe Video Transmission" aims to develop a robust framework for secure video communication in the face of evolving quantum computing threats. This initiative focuses on integrating cutting-edge quantum cryptography techniques with classical encryption methods to enhance the security and integrity of video data during transmission. Utilizing Shamir's Secret Sharing for secure key distribution, the framework enables user authentication, video encryption, and watermark embedding while ensuring data confidentiality. Users can register, log in, and upload videos with embedded watermarks for processing. The cryptography library is employed to encrypt each uploaded video, with key shares stored separately to prevent unauthorized access. Encrypted video frames are stored for later retrieval, and the decryption process involves reassembling key shares to reconstruct the original video while extracting watermarks from the first frame. The project leverages OpenCV for efficient video processing and incorporates secure file handling techniques to protect sensitive data. Ultimately, this project offers a user-friendly interface alongside robust backend encryption mechanisms, aiming to provide a significant advancement in the field of secure video transmission in a post-quantum world.

Methodologies

Modules Name:

Modules Name:

- User Authentication Module
- Video Upload Module
- Encryption Module
- Video Processing Module
- Decryption Module

Modules Explanation:

User Authentication Module

The User Authentication Module serves as the gateway for users to access the application, ensuring that only authorized individuals can upload and manage video content. This module includes a registration system where new users can create accounts by providing essential information, such as username and password, which are securely hashed for protection. Additionally, the login functionality validates user credentials against stored records, allowing for session management that maintains user login status throughout their interaction with the application. By implementing robust authentication mechanisms, this module enhances the security of user accounts and protects sensitive data from unauthorized access.

Video Upload Module

The Video Upload Module facilitates the seamless process of uploading video files along with optional watermarks. Users can easily select video files from their devices through a user-friendly interface, which includes file type and size validation to ensure compatibility with the system requirements. This module also allows users to input watermark information, which will be embedded into the video during processing. By streamlining the upload process and ensuring data integrity, this module serves as a crucial component in preparing videos for secure encryption and transmission.

Encryption Module

The Encryption Module is responsible for implementing advanced cryptographic techniques to secure uploaded video files. Utilizing both classical encryption methods and quantum-safe algorithms, this module encrypts videos to protect them from unauthorized access during transmission. A key feature of this module is the incorporation of Shamir's Secret Sharing, which divides the encryption keys into multiple shares for enhanced security and safe distribution. This ensures that no single entity has access to the complete key, significantly mitigating the risk of key compromise. By leveraging robust encryption practices, this module guarantees the confidentiality and integrity of video data.

Video Processing Module

The Video Processing Module employs OpenCV to perform various tasks related to video frames, enhancing the overall functionality of the application. This module is responsible for extracting individual frames from uploaded videos, manipulating them as needed, and embedding watermarks into the appropriate frames. It also manages video format conversions and compressions to optimize performance and storage. By utilizing advanced image processing techniques, this module ensures that videos are processed efficiently while maintaining high quality, enabling secure handling of video content.

Decryption Module

The Decryption Module allows users to retrieve their uploaded videos securely by decrypting the previously encrypted files. This module employs a systematic approach to reassemble key shares, utilizing Shamir's Secret Sharing to reconstruct the original encryption key. Once the key is reconstructed, the module facilitates the decryption process, enabling users to access their original videos. Additionally, it extracts watermarks from the decrypted video, ensuring that users can verify their ownership and integrity. By providing a secure and efficient decryption process, this module enhances the overall user experience while maintaining data security.

Technique Used or Algorithm Used

Existing Technique: -

The existing system for video transmission primarily relies on traditional encryption techniques, such as symmetric and asymmetric algorithms (e.g., AES, RSA), to secure video data. While these methods effectively ensure confidentiality, integrity, and authenticity, they face significant challenges due to advancing computing capabilities that make them more vulnerable to brute-force and cryptographic attacks. Additionally, the increasing demand for security in digital communication necessitates stronger encryption methods. Many systems currently utilize SSL (Secure Sockets Layer) for secure transmission over the internet, adding a layer of protection; however, this approach may not be sufficient against sophisticated threats. Consequently, the limitations of existing methods highlight the urgent need for more advanced solutions, such as the proposed Hybrid Quantum Video Encryption Framework, to enhance the security of video transmission effectively.

- With the rise of more powerful computing technologies, traditional encryption methods face vulnerabilities, as they can be subjected to brute-force attacks and other cryptographic attacks.
- **Drawbacks: -**
- **Vulnerability to Attacks:** Traditional encryption methods are increasingly susceptible to brute-force and cryptographic attacks due to advancing computational power.
- **Quantum Computing Threat:** The rise of quantum computing poses a significant risk to the security of conventional encryption algorithms.
- **Inadequate Security Measures:** SSL/TLS, while providing a layer of security, may not fully protect against sophisticated cyber threats.
- **Performance Limitations:** Traditional encryption algorithms can experience performance bottlenecks when handling large volumes of video data

Proposed Technique Used or Algorithm Used:

The proposed system is a Flask-based web application designed to deliver secure video processing, encryption, and watermark embedding, with a strong focus on user authentication and data confidentiality. This platform allows users to register, log in,

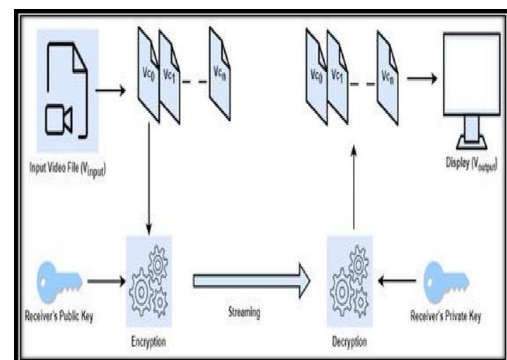
and upload video files, along with watermark images, to enhance security and content integrity. Video files are encrypted, and the encryption key is split using Shamir's Secret Sharing technique, ensuring both secure distribution and controlled access to the decryption key. This process of splitting and securing the encryption key guarantees that only authorized users with the required number of key shares can successfully decrypt and reconstruct the video.

Once uploaded, each video undergoes watermark embedding using OpenCV, where the watermark is integrated into each frame. Following this, the watermarked frames are encrypted frame by frame, allowing for individual frame retrieval and flexible management of video data. The encrypted frames are stored separately, making the data accessible only through the reconstruction and decryption processes. This frame-by-frame encryption further ensures that no single frame is exposed in the absence of the full decryption key, enhancing the overall security of the system.

Advantages: -

- **Comprehensive Library:** OpenCV offers a wide range of functions and tools for image and video processing, making it suitable for various computer vision tasks.
- **Real-Time Processing:** OpenCV is optimized for real-time applications, enabling fast processing of images and videos, which is crucial for time-sensitive tasks.
- **Ease of Use:** With a user-friendly API and extensive documentation, OpenCV simplifies the development of complex computer vision applications.
- **Scalable Security:** The scheme can easily scale to accommodate any number of participants and shares without compromising security

System Architecture:



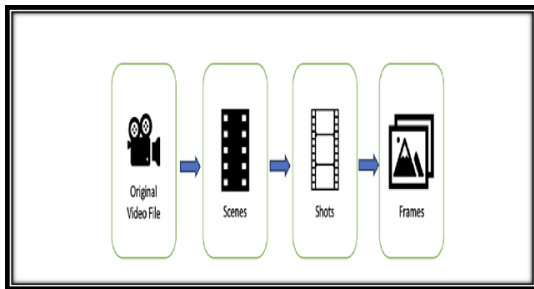


Fig -System Architecture

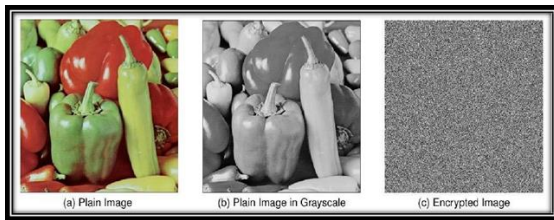


Fig -Shows the Encryption Process of Image

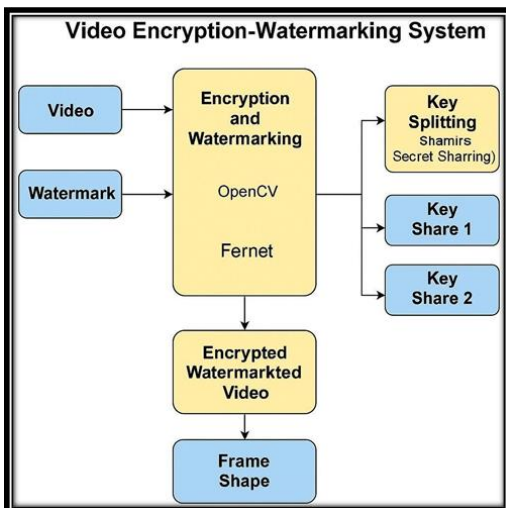


Fig- Advanced Encryption for Quantum-Safe Video Transmission

III. SNAPSHOTS

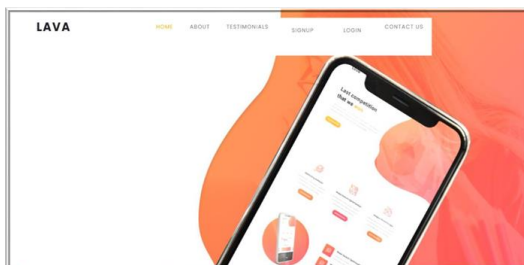


Fig: 3.1 Home Page

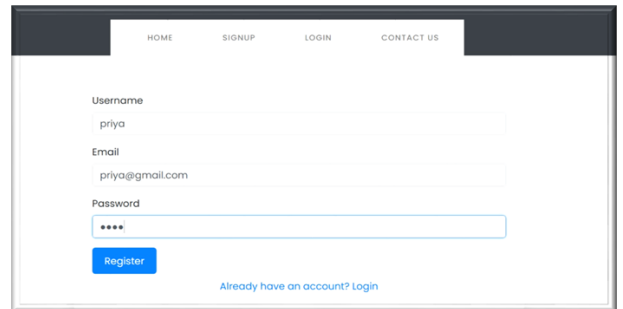


Fig: 3.2 Register Page

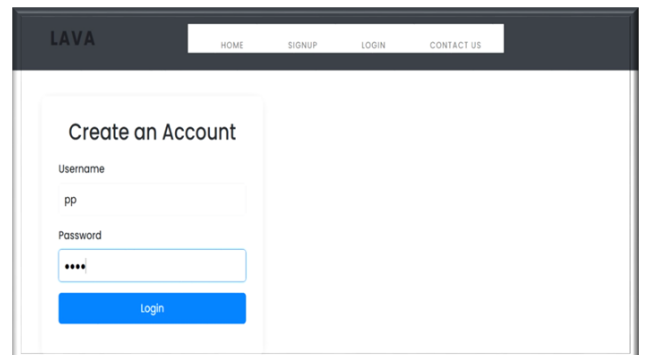


Fig: 3.3 Login Page

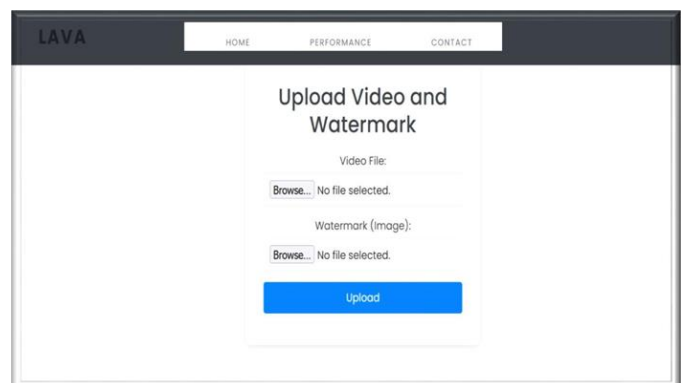


Fig: 3.4 Upload Video & Watermark

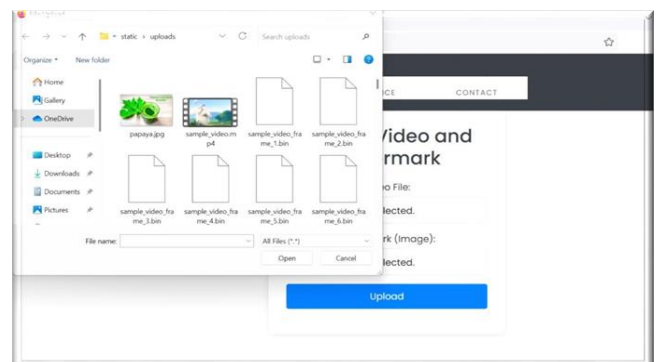


Fig: 3.5 Select Video & Watermark

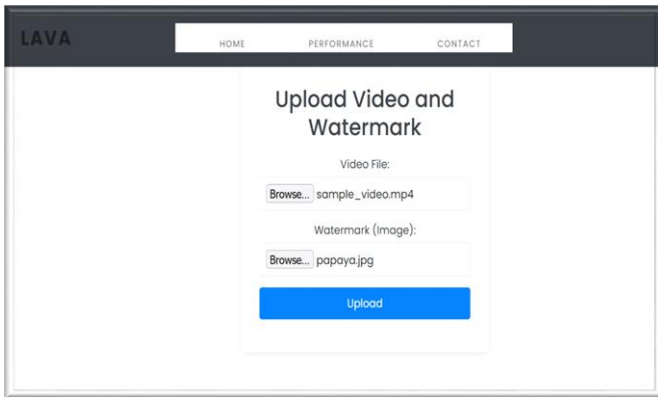


Fig: 3.6 Successful Uploaded

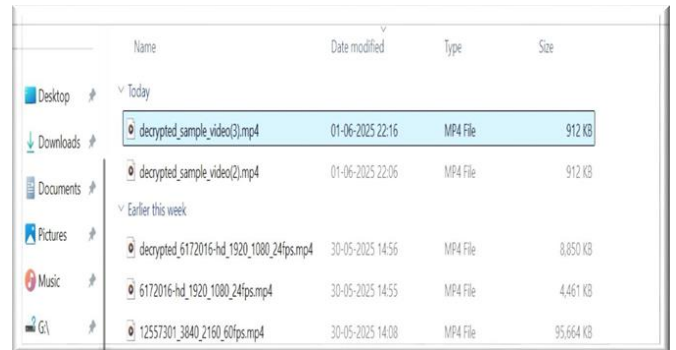


Fig:3.9 Open Decrypted Video

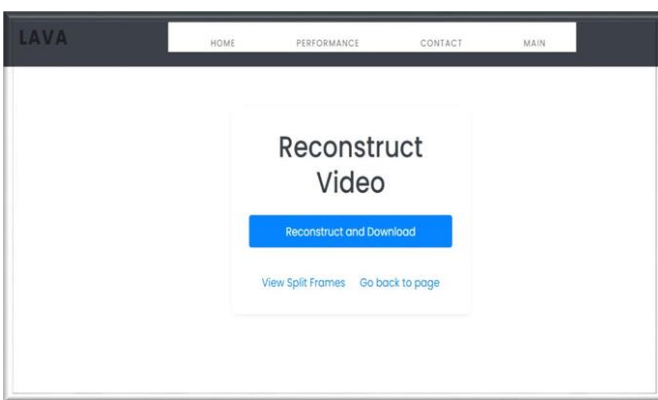


Fig: 3.7 Reconstruct Video



Fig: 3.10 Video with Watermark

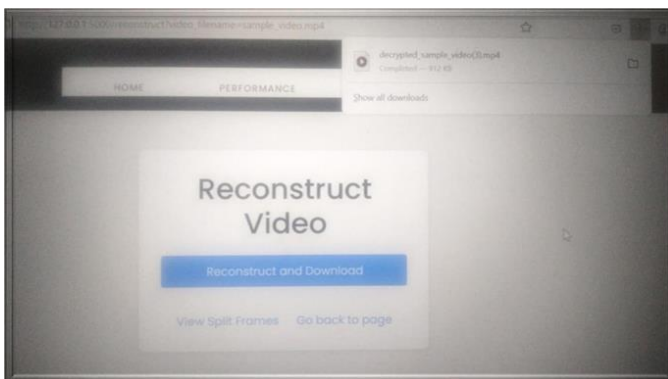


Fig: 3.8 Download Video

IV. SOFTWARE TESTING

General

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product. It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement.

Acceptance testing for Data Synchronization:

- The Acknowledgements will be received by the Sender Node after the Packets are received by the Destination Node
- The Route add operation is done only when there is a Route request in need
- The Status of Nodes information is done automatically in the Cache Updation process

Build the test plan

Test Case ID	Module	Test Scenario	Input	Expected Output	Actual Output	Status
01	Video Upload	Upload a valid video file	Sample.mp4	Video uploaded successfully	Video uploaded successfully	✓ Pass
02	Encryption Module	Encrypt uploaded video	Sample.mp4	Encrypted file generated	Encrypted file generated	✓ Pass
03	Decryption Module	Decrypt video with correct key	Encrypted.mp4 + Correct Key	Original video restored	Original video restored	✓ Pass
04	Decryption Module	Attempt decryption with incorrect key	Encrypted.mp4 + Wrong Key	Error: Invalid decryption key	Garbage output, unreadable video	✗ Fail
05	Video Upload	Upload an unsupported file format	Sample.txt	Error: Unsupported format	System crashed, no error shown	✗ Fail

V. FUTURE ENHANCEMENT FUTURE ENHANCEMENTS

Future enhancements for the "Advanced Encryption for Quantum-Safe Video Transmission" project could include several key improvements to further bolster its functionality and security. Integrating machine learning algorithms could enable the system to monitor video uploads and transmissions for anomalous behavior, enhancing threat detection capabilities. Additionally, incorporating block chain technology would provide tamper-proof storage for encrypted videos and key shares, increasing user trust and data integrity. Implementing real-time encryption and decryption could expand the project's applicability to live video streaming and conferencing. Enhancing user role management would allow for specific access permissions based on roles, while supporting a wider range of video formats and codes would cater to diverse user needs. Continuous improvements to the user interface would enhance user experience, and integrating advanced watermarking techniques would provide robust ownership verification. Optimization for performance and scalability would ensure the application can handle larger volumes of data efficiently. Incorporating multi-factor authentication would

significantly strengthen user security, while cloud integration would offer scalable storage solutions for convenient data retrieval. Finally, enhancing cross-platform compatibility would allow users to engage with the application across various devices, and providing comprehensive training materials would empower users to maximize their utilization of the system. Collectively, these enhancements would position the project to effectively address the evolving challenges in secure video transmission.

VI. CONCLUSION

In conclusion, the "Advanced Encryption for Quantum-Safe Video Transmission" project represents a significant advancement in the realm of secure video processing and transmission. By leveraging a hybrid approach that combines classical encryption techniques with innovative quantum-safe methodologies, the project effectively addresses the growing need for robust security measures in the digital communication landscape. The modular design of the application enhances its functionality, allowing for seamless user authentication, video upload, encryption, and processing, while ensuring data confidentiality and integrity. Future enhancements, such as the integration of machine learning for anomaly detection, for

tamper- proof storage, and real-time encryption capabilities, promise to further strengthen the system's security and usability. As digital communication continues to evolve, this project not only meets current security demands but also positions itself as a forward-thinking solution capable of adapting to future challenges in video transmission. Ultimately, by providing users with a secure and user-friendly platform for video encryption, this project contributes to safeguarding sensitive visual data and promoting trust in digital communication systems.

REFERENCES

1. Thabit, Fursan, Ozgu Can, Asia Othman Aljahdali, Ghaleb H. Al-Gaphari, and Hoda A. Alkhzaimi. "A Comprehensive Literature Survey of Cryptography Algorithms for Improving the IoT Security." *Internet of Things* (2023): 100759.
2. Hariprasad, Yashas, K. J. Latesh Kumar, L. Suraj, and S. S. Iyengar. "Boundary-Based Fake Face Anomaly Detection in Videos Using Recurrent Neural Networks." In *Proceedings of SAI Intelligent Systems Conference*, pp. 155-169. Cham: Springer International Publishing, 2022.
3. Mohseni, Masoud, Peter Read, Hartmut Neven, Sergio Boixo, Vasil Denchev, Ryan Babbush, Austin Fowler, Vadim Smelyanskiy, and John Martinis. "Commercialize quantum technologies in five years." *Nature* 543, no. 7644 (2017): 171-174.
4. Thejas, G. S., Yashas Hariprasad, S. S. Iyengar, N. R. Sunitha, Prajwal Badrinath, and Shasank Chennupati. "An extension of Synthetic Minority Oversampling Technique based on Kalman filter for imbalanced datasets." *Machine Learning with Applications* 8 (2022): 100267.
5. Zhu, Dexin, Jun Zheng, Hu Zhou, Jianan Wu, Nianfeng Li, and Lijun Song. "A hybrid encryption scheme for quantum secure video conferencing combined with blockchain." *Mathematics* 10, no. 17 (2022): 3037.
6. Gisin, Nicolas, Gr'egoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. "Quantum cryptography." *Reviews of modern physics* 74, no. 1 (2002): 145.
7. Wootters, William K., and Wojciech H. Zurek. "The no-cloning theorem." *Physics Today* 62, no. 2 (2009): 76-77.
8. Scarani, Valerio, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Du'sek, Norbert L'utkenhaus, and Momtchil Peev. "The security of practical quantum key distribution." *Reviews of modern physics* 81, no. 3 (2009): 1301.