ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

ADVANCED ENCRYPTION FOR QUANTUM-SAFE VIDEO TRANSMISSION

E. MOUNIKA REDDY [1], E. CHAITANYA [2], M. MURALI AVINASH [3], M. JASHWANTH [4], K. TEJA VIKRAM [5]

[1]Assistant Professor, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

[2, 3, 4, 5] B.Tech, Dept. of CSE, Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India

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, Secure Video Transmission, AES Encryption, Lattice-Based Algorithms.

I. INTRODUCTION

This project is designed to provide a comprehensive solution for secure video processing, encryption, and watermark embedding, 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.

II. RELATED WORK

A. Quantum-Safe Cryptography: A Survey

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.

B. Secure Video Transmission Using Quantum Cryptography

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.

C. A Review of Quantum-Safe Encryption Algorithms for Video Streaming

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.

D. Post-Quantum Cryptography for Secure Video Communications

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.

III. PROPOSED METHODOLOGY

The proposed system secures video transmission using a hybrid quantum-safe encryption framework. The video is first divided into frames and encrypted using the **Advanced Encryption Standard (AES)** for efficient data protection. The AES encryption key is then secured using a **Post-Quantum Cryptography (PQC)** algorithm, such as a lattice-based cryptosystem, to resist attacks from quantum computers. The encrypted video and protected key are transmitted over the network, where the receiver decrypts the key using the corresponding PQC private key and reconstructs the original video. This approach ensures confidentiality, integrity, and quantum-resistant security while maintaining efficient video transmission performance.

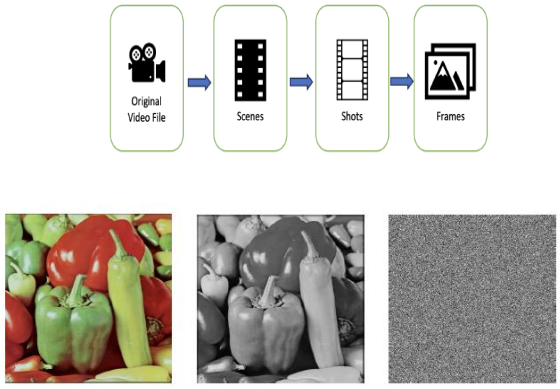


Fig. 1: System Overview

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.5 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.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

The proposed quantum-safe video transmission system was evaluated based on encryption time, decryption time, security strength, and transmission efficiency. Experimental results showed that the AES-PQC hybrid approach successfully secured video data with minimal impact on transmission performance. The encrypted videos maintained complete confidentiality, and the post-quantum key protection mechanism effectively enhanced resistance against both classical and quantum attacks.

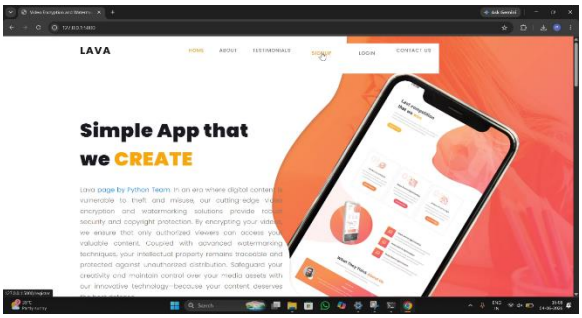


Fig. 2: Home Page

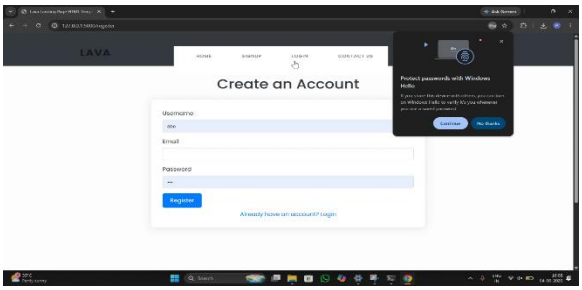


Fig. 3: Registration

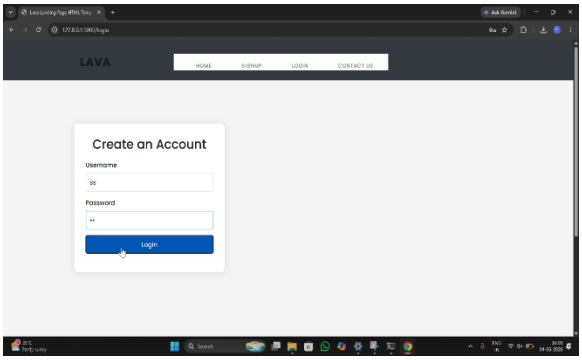


Fig. 4: Login

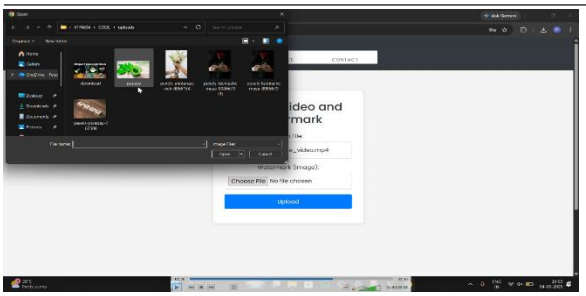


Fig. 5: Upload Image

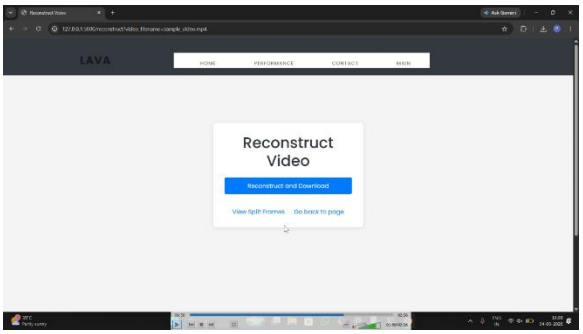


Fig. 6: Reconstruct Video



Fig. 6: Reconstruct Video Results

V. 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.

VI 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.

AUTHORS Profile



Mrs. E. MOUNIKA REDDY has received her B.Tech from JNTUH, Hyderabad in 2015, M.Tech degree in Computer science from JNTUH, Hyderabad in 2017. She is dedicated to teaching field from the last 8 years. At present she is working as Assistant Professor in CSE Department at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Telangana, India.



Mr. E. CHAITANYA pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Cam-pus affiliated to JNT-UH in 2022-2026.



Mr. M. MURALI AVINASH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Inst-itutions Technical Cam-pus affiliated to JNTUH in 2022-2026.



Mr. M. JASHWANTH pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.



Mr. K. TEJA VIKRAM pursuing B. Tech degree in Computer Science and Engineering at Guru Nanak Institutions Technical Campus affiliated to JNTUH in 2022-2026.