IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 3, May-June 2025

Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203126

Safe Video Transmission through Advanced Cryptography

P. Bhargav, P. Yashwanth, P. Bhagya Laxmi, S. Sivasankara Rao

Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, 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.

I. INTRODUCTION

1. GENERAL

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. 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.

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

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203126

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.

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.

PROBLEM STATEMENT

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 sophisticatedthreats.

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. 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.

II. EXISTING SYSTEM

- 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.

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.

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203126

III. LITERATURE SURVEY

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.

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

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.

1q**APPLICATION GENERAL**

Project Safe Video Transmission through Advanced Cryptography aims to secure video data during transmission, making it resistant to unauthorized access, tampering, and interception by employing sophisticated cryptographic techniques, often combined with steganography. This project finds critical applications across diverse sectors. In secure video conferencing and communication, it is vital for government and military communications to transmit classified briefings, strategic discussions, and surveillance footage securely, while in corporate and business settings, it protects sensitive company information and intellectual property during meetings. Healthcare telemedicine relies on it to ensure patient data privacy, and individuals use it for end-to-end encrypted video calls to safeguard their privacy.

IV. FUTURE ENHANCEMENT

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.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 8.152| A Bi-Monthly, Double-Blind Peer Reviewed & Refereed Journal |

|| Volume 12, Issue 3, May - June 2025 ||

DOI:10.15680/IJARETY.2025.1203126

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.

REFERENCE

[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.

[9] Yang, Yu-Guang, Juan Xia, Xin Jia, and Hua Zhang. ”Novel image encryption/decryption based on quantum Fourier transform and double phase encoding.” Quantum information processing 12 (2013): 3477-3493.

[10] Tan, Ru-Chao, Tong Lei, Qing-Min Zhao, Li-Hua Gong, and Zhi-Hong Zhou. ”Quantum color image encryption algorithm based on a hyperchaotic system and quantum Fourier transform.” International Journal of Theoretical Physics 55 (2016): 5368-5384.

[11] Sharma, Deepak. ”Robust technique for image encryption and decryption using discrete fractional Fourier transform with random phase masking.” Procedia Technology 10 (2013): 707-714.

[12] Kordov, Krasimir, and Georgi Dimitrov. ”A new symmetric digital video encryption model.” Cybernetics and Information Technologies 21, no. 1 (2021): 50-61.

[13] Yan, Fei, Abdullah M. Iliyasu, Salvador E. Venegas-Andraca, and Huamin Yang. ”Video encryption and decryption on quantum computers.” International Journal of Theoretical Physics 54 (2015): 2893-2904.

[14] Zhou, Nan Run, Tian Xiang Hua, Li Hua Gong, Dong Ju Pei, and Qing Hong Liao. ”Quantum image encryption based on generalized Arnold transform and double random-phase encoding.” Quantum Information Processing 14 (2015): 1193-1213.

[15] Hu, Wen-Wen, Ri-Gui Zhou, Jia Luo, She-Xiang Jiang, and Gao-Feng Luo. ”Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms.” Quantum Information Processing 19 (2020): 1-29.

[16] Li, Chunmeng, and Xiaozhong Yang. ”An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos.” Optik 260 (2022): 169042.

[17] PSong, Xianhua, Guanglong Chen, and Ahmed A. Abd El-Latif. ”Quantum color image encryption scheme based on geometric transformation and intensity channel diffusion.” Mathematics 10, no. 17 (2022): 3038

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 8.152

www.ijarety.in editor.ijarety@gmail.com