International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

Advanced Encryption For Quantum-Safe Video Transmission

CH.Gopi, Hithaishi Gajulapalli, Mohitha Vinnakota, Geenukunta Manish Kumar Goud

[1]Assistanat Professor, Department of Information Technology, Guru Nanak Institutions Technical Campus, India.

[2,3,4]B.Tech Students, Department of Information Technology, Guru Nanak Institutions Technical Campus, 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.

1-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.

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.

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.

2-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.

3-PROJECT DESCRIPTION:

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

1. User Authentication Module
SYSTEM ARCHITECTURE:

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.

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. 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.

4-DESIGN ENGINEERING

Design Engineering deals with the various UML [Unified Modelling language] diagrams for the implementation of project. Design is a meaningful engineering representation of a thing that is to be built. Software design is a process through which the requirements are translated into representation of the software. Design is the place where quality is rendered in software engineering.

International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 13, Issue 2, 2025

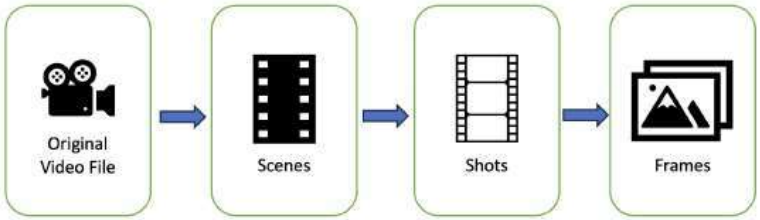
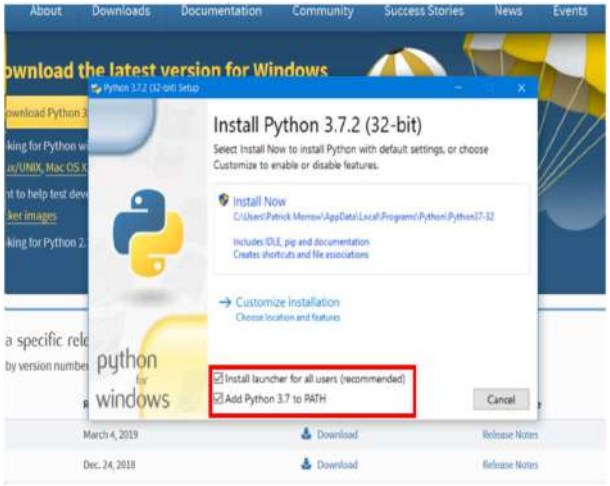
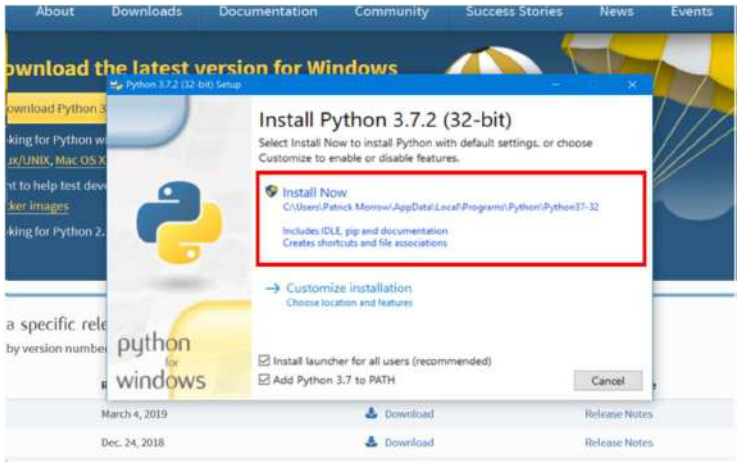


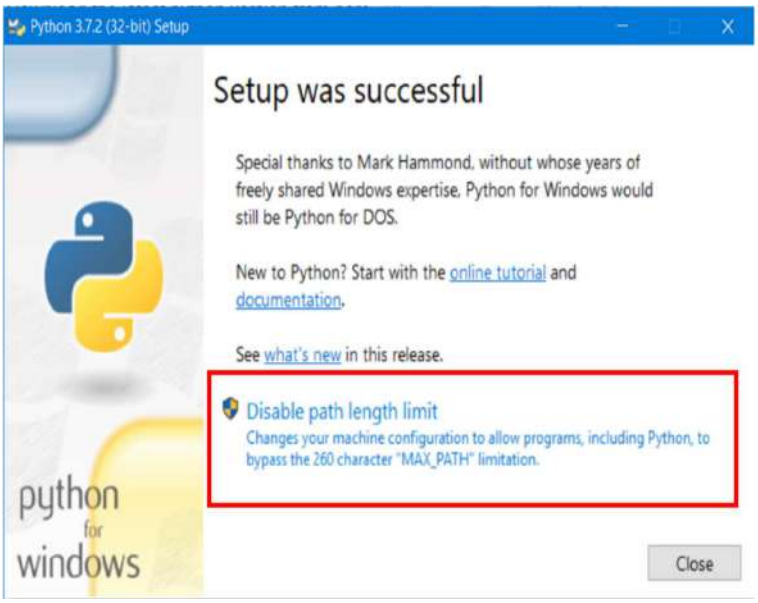
Fig 4.11: System Architecture

5-DEVELOPMENT TOOLS



International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 13, Issue 2, 2025





6-SOFTWARE TESTING

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.

Unit testing:

Unit testing involves the design of test cases that validate that the internal program logic is functioning properly, and that program input produce valid outputs. All decision branches and internal code flow should be validated. It is the testing of individual software units of the application .it is done after the completion of an individual unit before integration. This is a structural testing, that relies on knowledge of its construction and is invasive. Unit tests perform basic tests at component level and test a specific business process, application, and/or system configuration. Unit tests ensure that each unique path of a business process performs accurately to the documented specifications and contains clearly defined inputs and expected results.

Functional test:

Functional tests provide systematic demonstrations that functions tested are available as specified by the business and technical requirements, system documentation, and user manuals.

Functional testing is centered on the following items:

Valid Input : identified classes of valid input must be accepted.

Invalid Input : identified classes of invalid input must be rejected.

Functions : identified functions must be exercised.

Output : identified classes of application outputs must be exercised.

Systems/Procedures: interfacing systems or procedures must be invoked.

System Test

System testing ensures that the entire integrated software system meets requirements. It tests a configuration to ensure known and predictable results. An example of system testing is the configuration oriented system integration test. System testing is based on process descriptions and flows, emphasizing pre-driven process links and integration points.

Integration Testing:

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects.

The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

7-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.

[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.
[18] Wang, Shen, Xianhua Song, and Xiamu Niu. "A novel encryption algorithm for quantum images based on quantum wavelet transform and diffusion." In Intelligent Data analysis and its Applications, Volume II: Proceeding of the First Euro-China Conference on Intelligent Data Analysis and Applications, June 13-15, 2014, Shenzhen, China, pp. 243-250. Springer International Publishing, 2014.
[19] Wang, Han, Jian Wang, Ya-Cong Geng, Yan Song, and Ji-Qiang Liu."Quantum image encryption based on iterative framework of frequencyspatial domain transforms." International Journal of Theoretical Physics 56 (2017): 3029-3049.
[20] Gong, Li-Hua, Xiang-Tao He, Shan Cheng, Tian-Xiang Hua, and Nan-Run Zhou. "Quantum image encryption algorithm based on quantum image XOR operations." International Journal of Theoretical Physics 55 (2016): 3234-3250.
[21] Wang, Jian, Ya-Cong Geng, Lei Han, and Ji-Qiang Liu. "Quantum image encryption algorithm based on quantum key image." International Journal of Theoretical Physics 58 (2019): 308-322.
[22] Jose, M. Victor, and V. Seenivasagam. "An Enhanced Opass With Modified Elliptic Curve Cryptography-Based User Authentication Scheme For Grid Computing." Life Science Journal 10, no. 3 (2013).
[23] Le, Phuc Q., Abdullahi M. Iliyasu, Fangyan Dong, and Kaoru Hirota."A flexible representation and invertible transformations for images on quantum computers." New Advances in Intelligent Signal Processing (2011): 179-202.
[24] Jiang, Nan, and Luo Wang. "Quantum image scaling using nearest neighbor interpolation." Quantum Information Processing 14 (2015):1559-1571.
[25] Sun, Bo, A. Iliyasu, Fei Yan, Fangyan Dong, and Kaoru Hirota. "An RGB multi-channel representation for images on quantum computers." J.Adv. Comput. Intell. Intell. Inform 17, no. 3 (2013).