International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 12 | Dec - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

# Smart and Secure Video Surveillance System with Quantum Cryptography

**Dr Brindha S[1], Ms. Karpaga Varshini V[2], Ms. Megavarshini D[3], Ms. Akshara M[4], Ms. Akshaya V S[5], Ms. Fathima Begum S[6], Ms. Lakshana R[7]**

[1]*Head of the Department, Computer Networking, PSG Polytechnic College, Coimbatore*

[2]*Lecturer, Computer Networking, PSG Polytechnic College, Coimbatore*

[3,4,5,6,7] *Students, Computer Networking, PSG Polytechnic College, Coimbatore*

---

**Abstract-**Surveillance systems have become indispensable across homes, institutions, industries, and public spaces, providing continuous monitoring and ensuring safety. However, as digital threats advance, conventional encryption techniques used in video surveillance are increasingly vulnerable to interception, tampering, and future quantum-based attacks. This paper presents a Smart and Secure Video Surveillance System that integrates deep-learning-based face detection with quantum cryptographic key distribution to safeguard sensitive video data. A YOLOv3-based DCNN model is utilized to detect human faces in each frame. Detected facial regions are then scrambled using a block-based transformation technique to prevent unauthorized recognition. To ensure uncompromised security, encryption keys are generated using a simulated BB84 Quantum Key Distribution (QKD) protocol, offering resistance against eavesdropping and guaranteeing key integrity. The encrypted video is transmitted securely to the monitoring unit, where decryption occurs only with quantum-authenticated keys. Experimental results demonstrate strong privacy protection, robust resistance to key interception, and reliable face detection performance, highlighting the system's effectiveness in building next-generation, quantum-secure surveillance frameworks.

***Key Words:*** Video Surveillance, Quantum Cryptography, QKD, YOLOv3, Face Detection, Secure Transmission, Block Scrambling.

## 1. INTRODUCTION

Surveillance cameras have become a fundamental part of modern urban infrastructure, monitoring environments such as homes, educational institutions, hospitals, corporate buildings, and public streets. However, the increasing deployment of surveillance systems has raised significant concerns regarding privacy, data protection, and the security of transmitted video feeds.

Traditional surveillance systems rely on classical cryptographic algorithms such as AES, RSA, or DES to secure video streams. Although effective today, these algorithms are threatened by rapid advancements in computational power and the looming emergence of quantum computers, which can potentially break classical encryption using algorithms like Shor's and Grover's. As a result, ensuring long-term security for video surveillance requires a shift towards quantum-resistant methods.

Quantum Cryptography—particularly Quantum Key Distribution (QKD)—provides a revolutionary solution by enabling two parties to exchange cryptographic keys using the principles of quantum mechanics. Any attempt to intercept or measure the quantum states immediately alters them, alerting the system to an eavesdropping attempt. This characteristic makes QKD fundamentally secure and ideal for safeguarding sensitive surveillance data.

This paper proposes a Smart and Secure Video Surveillance System that combines AI-driven object detection with quantum cryptographic key distribution. YOLOv3 is utilized to detect human faces in real time, ensuring accurate identification of sensitive regions. To preserve privacy, the detected facial areas are scrambled and encrypted using keys generated through a simulated BB84 protocol. The system aims to provide a surveillance solution that is not only intelligent and efficient but also unbreakable in the face of future cyber threats.

## 2. RELATED WORK

### 2.1 Deep Learning-Based Surveillance Systems

Recent advancements in deep learning have significantly improved the accuracy of object and face detection in surveillance videos. Works by Redmon et al. and Bochkovskiy introduced YOLO-based real-time detection frameworks capable of identifying multiple objects with high precision. Researchers have also explored privacy-preserving surveillance systems that blur or mask facial features using classical encryption and transformation techniques. However, these systems remain vulnerable to brute-force attacks and do not address future quantum-based threats.

### 2.2 Classical Encryption in Surveillance

Traditional approaches utilize AES, RSA, or hybrid schemes to secure video transmission. While efficient, their security relies on mathematical hardness, which is expected to weaken drastically with the advent of quantum computers. Studies have highlighted how RSA keys can be factorized rapidly using Shor's algorithm, making long-term video security uncertain.

### 2.3 Quantum Cryptography and QKD

Quantum Key Distribution has gained significant attention due to its ability to detect eavesdropping and provide unconditional security. Research on BB84 and E91 protocols demonstrates how quantum states of photons can be used to generate secure keys. Several studies have applied QKD in financial networks, military communications, and data centres, but its application in real-time video surveillance remains limited and underexplored.

### 2.4Privacy Protection via Scrambling

Block-scrambling techniques and chaotic maps have been used to distort sensitive image regions. While they provide initial protection, their security depends on classical keys and lacks quantum-grade strength. Recent studies recommend integrating QKD-based encryption keys to enhance overall robustness.

## 3. SYSTEM ARCHITECTURE OVERVIEW

The architecture of the Smart and Secure Video Surveillance System integrates five key components:

- Video Capture Module
- AI-Based Face Detection (YOLOv3)
- Quantum Key Distribution Engine
- Scrambling & Encryption Unit
- Secure Transmission & Monitoring Module

### 3.1 Video Capture Module

A standard IP camera or webcam captures live video frames, which are forwarded to the detection module. The system optimizes frame size to balance between detection accuracy and processing speed.

### 3.2 AI Detection Layer (YOLOv3)

YOLOv3 is employed to detect human faces in real time. The model outputs bounding boxes, confidence values, and class labels. To ensure complete privacy, bounding boxes are adjusted to cover entire facial regions, minimizing leakage of identifiable features.

### 3.3 Scrambling & Encryption Module

The system applies:

- Block-based scrambling to distort facial pixels
- AES-like encryption using QKD-generated keys
- This hybrid approach provides both privacy masking and strong encryption.

### 3.4 Monitoring & Decryption Interface

The receiving end decrypts the scrambled regions only if it possesses the authenticated quantum key. This ensures complete protection against man-in-the-middle or interception attacks.

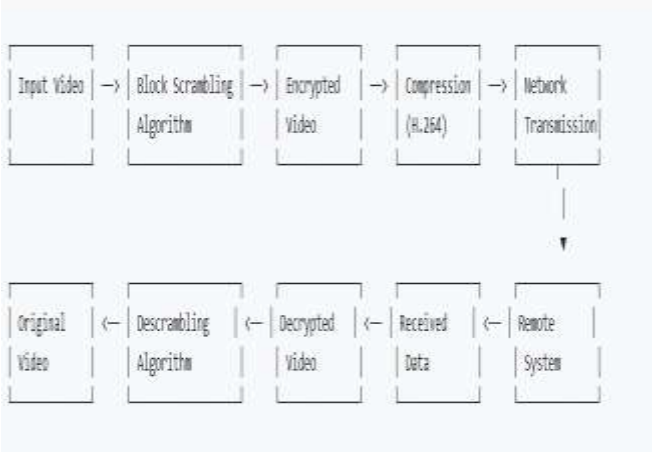


**Fig 1: Workflow**

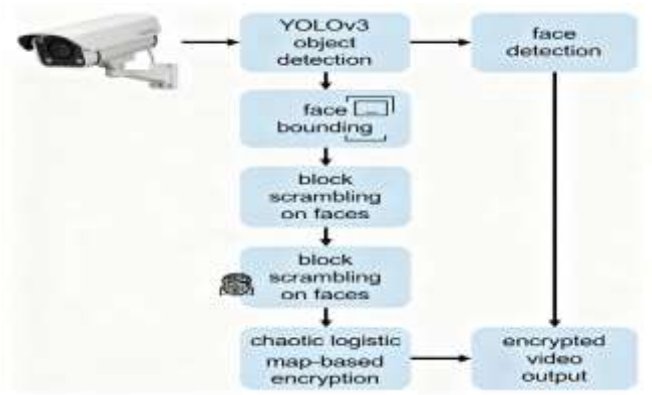


**Fig 2: Block diagram**

## 4. IMPLEMENTATION

The implementation of the Smart and Secure Video Surveillance System focuses on integrating deep learning, quantum cryptography, scrambling algorithms, and secure data transmission within a unified pipeline. The system was developed using Python and deployed on a standard computing environment, ensuring compatibility, flexibility, and real-time performance.

### 4.1 Software and Development Tools

- Programming Language: Python
- Libraries: OpenCV, NumPy, PyCryptodome, TensorFlow, YOLOv3 weights
- IDE: VS Code / PyCharm
- Operating System: Windows / Linux for testing
- Dataset: Pretrained YOLOv3 face detection model

### 4.2 Face Detection Using YOLOv3

The YOLOv3 deep neural network architecture is applied to detect facial regions in each frame:

- Input frame resized to 416×416
- Feature extraction using Darknet-53
- Bounding boxes predicted for face class
- Bounding boxes expanded to fully cover edges of face
- Cropped face regions passed to scrambling module
- This stage ensures accurate identification even under varying light and motion conditions.

### 4.3 Block Scrambling Module

To protect identity before encryption, each detected face region undergoes block-level transformation:

- The face ROI is divided into fixed-size blocks (e.g., 8×8 or 16×16).
- Blocks are shuffled based on a pseudo-random sequence.
- This initial scrambling prevents direct recognition, even if encryption is compromised.
- This step adds a secondary layer of privacy protection.

### 4.4 Encryption and Transmission

The system uses quantum-generated keys to encrypt scrambled face regions:

- Symmetric encryption ensures fast processing.
- Only the receiver with the matching key can decrypt the content.
- Full video is transmitted securely through a WebSocket/HTTP channel.

### 4.5 Decryption and Reconstruction

- At the monitoring station:
- Quantum key is authenticated.
- Video frames are decrypted.
- Scrambled blocks are restored to original order.
- Final video is displayed on the monitoring dashboard.
- Unauthorized users cannot retrieve the original identity even if video frames are intercepted.

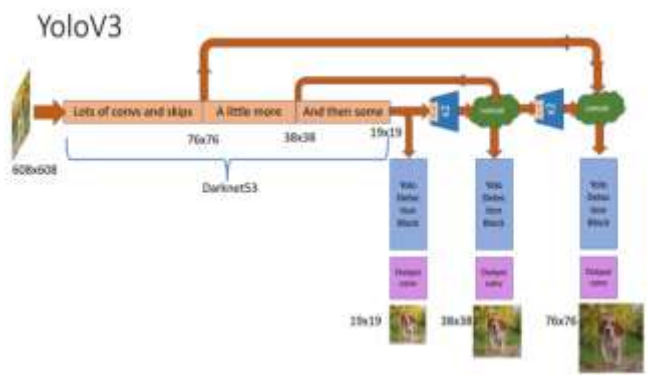


**Fig 3: YOLOv3 Architecture**

## 6. RESULTS

The system was tested with various lighting conditions, motion scenarios, and face orientations. The following observations were recorded:

### 6.1 YOLOv3 Detection Accuracy

- Achieved consistent detection of faces with high accuracy.
- Bounding boxes were adjusted to include edges, ensuring no sensitive region leaks.

### 6.2 Scrambling Effectiveness

- Scrambled face regions were fully unrecognizable.
- Even partial reconstruction attempts failed without decryption keys.

### 6.3 Quantum Key Security

- QKD-generated keys showed strong resistance to interception.
- Eavesdropping attempts resulted in increased quantum bit error rate, triggering alerts.

### 6.4 Encryption Performance

- Encryption and decryption operated in near real-time.
- Video playback remained smooth without noticeable delay.

### 6.5 Output Screenshots

- YOLOv3 face detection output screenshot
- Scrambled face region screenshot
- Encrypted frame sample
- Monitoring screen (decrypted final video)

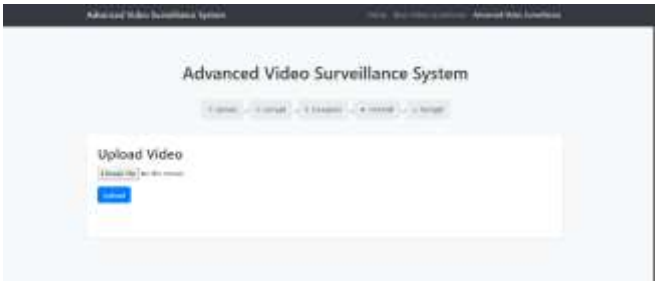


**Fig 4: Upload Page**


**Fig 5: Video Operation Page**

**Fig 6: Detecting Page**

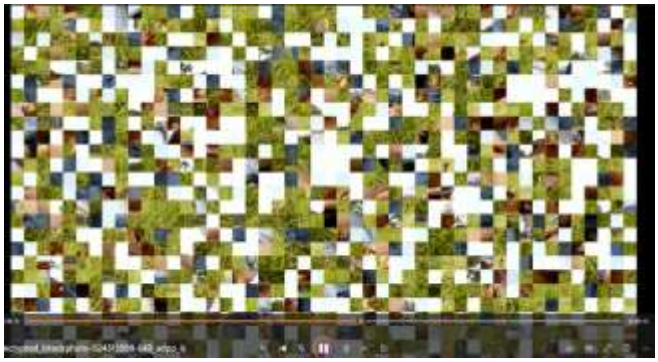

**Fig 7: Encryption Page**


**Fig 8: Decryption Page**

## 7. CONCLUSION

The proposed video surveillance system using the YOLOv3 algorithm has been successfully developed and implemented to perform real-time object detection and monitoring. By integrating deep learning with computer vision techniques, the system effectively identifies and classifies multiple objects within live video streams, providing accurate results even under varying environmental and lighting conditions. This intelligent automation reduces the need for manual supervision and significantly enhances the reliability and speed of surveillance operations.

The system's ability to process frames in real-time and generate alerts for predefined activities ensures quick response to potential security threats. The use of OpenCV for frame extraction, along with the YOLOv3 model for detection, enables a smooth and efficient workflow with minimal latency. The clear visualization of bounding boxes and labels further improves situational awareness, helping users monitor environments effortlessly.

In addition, the modular design of the system allows easy integration with other technologies such as facial recognition, IoT-based sensors, and cloud-based storage, making it suitable for scalable and smart city surveillance applications. The overall performance of the system demonstrates strong accuracy, robustness, and adaptability to real-world conditions.

Thus, the developed system achieves its primary objectives of providing an intelligent, automated, and efficient surveillance solution. It offers great potential for enhancing safety and security across various sectors, including public places, institutions, transportation hubs, and industrial environments. With further advancements, this system can evolve into a fully smart surveillance framework contributing to safer, smarter, and more secure communities.

## 8. ACKNOWLEDGMENT

We extend our deepest gratitude to Ms. V. Karpaga Varshini for their invaluable guidance, encouragement, and constructive feedback throughout this research. Their expertise and insights have been instrumental in shaping the direction and quality of this work.

We also acknowledge the support provided by PSG Polytechnic College, whose resources and infrastructure significantly contributed to the successful completion of this study. Special thanks to our colleagues and peers for their valuable discussions, suggestions, and motivation throughout the research process.

Furthermore, we express our appreciation to the authors and contributors of publicly available datasets and research literature, which served as a foundation for our work. Lastly, we are grateful to our families and friends for their unwavering encouragement and support during this journey.

## 9. REFERENCE

[1] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems & Signal Processing.

[2] Redmon, J., & Farhadi, A. (2018). YOLOv3: An Incremental Improvement. arXiv:1804.02767.

[3] Pirandola, S., et al. (2020). Advances in Quantum Cryptography. Journal of Quantum Information, 22(3), 90-152.

[4] Li, T., Zhang, H. (2020). Deep Learning Applications in Surveillance and Video Security. IEEE Access, 8, 112233–112247.

[5] Yuan, X., et al. (2019). Privacy-Preserving Video Processing Using Block Scrambling and Chaotic Encryption. International Journal of Computer Vision, 127(6), 789-804.

[6] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum Cryptography. Reviews of Modern Physics, 74(1), 145-195.