

## NATIONAL UNIVERSITY OF COMPUTER AND EMERGING SCIENCE

# Anomaly Detection in CCTV Footage Using AI

# Final year Project



## GROUP MEMBERS

**Name Roll No**

Shayan Ahmad 22F- 3816

Ali Naqvi 22F- 3806

Ishrat Fatima 22F- 3616

Aqsa Ijaz 22F- 3615

**Submitted To: Sir Iqbal Khan**

# Abstract

The **Anomaly Detection in CCTV Footage** system leverages AI to enhance security by identifying unusual activities or behavior in real-time. Designed for public safety, this platform processes CCTV footage using advanced algorithms to detect threats like violence, theft, or unauthorized access. It ensures proactive security measures by sending instant alerts to security personnel, thus reducing response time. By focusing on cutting-edge machine learning models and robust data processing, the system helps make surveillance more efficient, reliable, and scalable.

# Introduction

Modern surveillance systems face challenges like manual monitoring inefficiency, delayed response times, and increased false alarms. The **Anomaly Detection in CCTV Footage** system addresses these issues by integrating AI to automate and enhance the detection of suspicious activities. With real-time monitoring, pattern recognition, and anomaly classification, the system empowers security teams to act promptly. It provides a user-friendly interface, ensures high accuracy through advanced machine learning techniques, and protects sensitive data with robust security measures.

This system caters to public spaces like malls, airports, schools, and government buildings where constant vigilance is crucial. It integrates seamlessly with existing CCTV infrastructure to identify, analyze, and report anomalies effectively, thereby ensuring safety and reducing reliance on manual oversight.

# Goals and Objectives

# The Anomaly Detection in CCTV Footage system aims to:

* **Automate Threat Detection:** Utilize AI to identify anomalies such as intrusions, suspicious behavior, and emergencies in real-time.
* **Enhance Security Response:** Provide instant alerts to security personnel, enabling faster response to potential threats.
* **Reduce Manual Monitoring Effort:** Minimize human error and improve efficiency by automating footage analysis.
* **Provide Real-Time Insights:** Offer live notifications and detailed reports to security teams and management.
* **Ensure Scalability and Flexibility:** Design a system that adapts to various environments and supports multiple camera setups.
* **Ensure Data Privacy and Security:** Use encrypted communication and storage to protect footage and alerts from unauthorized access.

# Scope of the Project

The **Anomaly Detection in CCTV Footage** system will feature the following key components:

* **User Authentication:** Secure sign-up and log-in processes for authorized personnel, using multi-factor authentication.
* **Real-Time Anomaly Detection:** Employ AI models trained to detect unusual activities such as aggression, loitering, or abandoned objects.
* **Customizable Alert System:** Send real-time notifications via SMS, email, or mobile app for verified anomalies.
* **Data Visualization:** Provide a dashboard to review detected anomalies with timestamps and flagged footage.
* **Behavioral Analysis:** Classify anomalies based on predefined patterns like crowding, restricted area access, or sudden motion.
* **Integration with Existing CCTV Systems:** Ensure compatibility with different CCTV camera models and brands.
* **Event Logging and Reporting:** Maintain logs of detected anomalies, with options for exporting detailed reports.
* **Scalable AI Models:** Enable training with diverse datasets for improved accuracy in different environments.
* **Privacy Features:** Blur faces or sensitive areas in the footage to comply with privacy regulations when sharing data.
* **Offline Mode:** Store flagged anomalies locally in case of network outages, ensuring no data is lost.

# Initial Study and Work Done So Far

* **Research on Existing Solutions:** We explored technologies used in systems like Avigilon, BriefCam, and RealNetworks. These solutions focus on crowd behavior analysis, intrusion detection, and object tracking.
* **Consultation with Industry Experts:** We engaged with professionals working on public safety and AI to identify challenges like false positives, data security, and model adaptability.
* **Technology Exploration:** Evaluated AI frameworks (e.g., TensorFlow, PyTorch) for real-time processing, and OpenCV for video analysis.
* **Dataset Analysis:** Studied publicly available datasets (e.g., UCF-Crime, CCTV-Fights) to understand anomaly patterns and fine-tune detection models.
* **Challenges Identified:** Addressed issues like varying lighting conditions, camera angles, and overlapping objects to ensure model robustness.

# Future Work

**The Anomaly Detection in CCTV Footage project will focus on the following:**

* Developing a scalable architecture for processing and analyzing multiple video streams simultaneously.
* Enhancing AI algorithms to minimize false positives and improve anomaly classification.
* Implementing secure cloud-based storage for anomaly footage and alerts.
* Conducting extensive field tests in diverse environments to validate system performance.

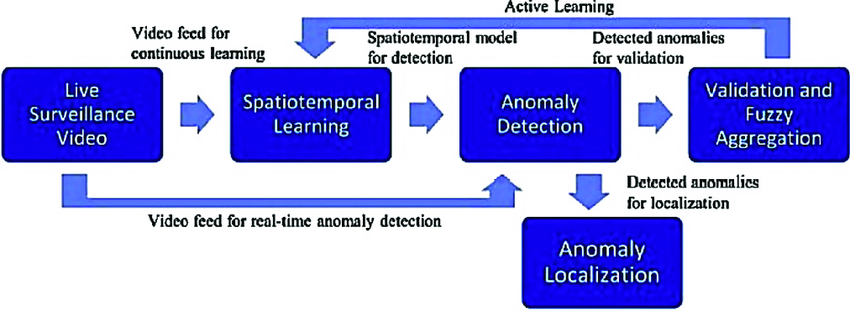
**How It Works**

1. **Data Collection and Preparation**:
   * **Video Data**: The model requires a substantial dataset of CCTV footage representing normal behavior (e.g., people walking, waiting, sitting) and a smaller set of unusual events (e.g., someone running, loitering in restricted areas, sudden gatherings).
   * **Annotation**: Anomalies in the footage are manually labeled to train the model on what constitutes "normal" and "abnormal" behavior.
2. **Preprocessing**:
   * **Frame Extraction**: Each video is broken down into individual frames so that actions can be analyzed frame-by-frame or in short sequences.
   * **Background Subtraction**: By isolating moving objects from the background, the model can focus on people and activities rather than static elements in the scene.
   * **Object Detection and Tracking**: The model detects and tracks objects (usually people and vehicles) in each frame, monitoring movement patterns and locations.
3. **Feature Extraction**:
   * **Spatial Features**: Characteristics like object position, size, speed, and direction are extracted to identify movement patterns.
   * **Temporal Patterns**: Using a sequence of frames, the model captures behaviors over time, which is essential for distinguishing routine activities from anomalies.
4. **Model Training**:
   * **Unsupervised Learning**: Since "anomaly" may vary by context, models like **autoencoders** or **clustering algorithms** (e.g., k-means) can be trained on normal patterns, learning what typical activities look like. When an event doesn’t fit these patterns, it’s flagged as unusual.
   * **Deep Learning Models**: Recurrent neural networks (RNNs), long short-term memory networks (LSTMs), or convolutional neural networks (CNNs) are commonly used to capture both spatial and temporal features in the footage.
   * **Anomaly Detection Algorithms**: Algorithms like one-class SVMs (support vector machines) or Gaussian mixture models (GMMs) are also popular for distinguishing anomalies from typical activities.
5. **Testing and Validation**: The model is tested on a separate dataset to evaluate its precision, recall, and false alarm rate. An effective model can detect genuine anomalies while minimizing false positives (ordinary events flagged as suspicious).
6. **Deployment**:
   * **Real-Time Monitoring**: The model can be integrated into a live CCTV system to analyze incoming footage in real-time, sending alerts to security personnel whenever an anomaly is detected.
   * **Post-Event Analysis**: The system can also be used to analyze archived footage, allowing investigators to review specific events or unusual behaviors in past footage.

**Comparison of Existing Websites/Apps**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Sr.# | Features | Anomaly detection in CCTV footage | Avigilon | BriefCam | RealNetworks |
| 1 | User Authentication (sign-up/login) | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 2 | Real-Time Anomaly Detection | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 3 | Customizable Alert System | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 4 | Data Visualization | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 5 | |  | | --- | |  |  |  | | --- | | Behavioral Analysis | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 6 | Integration with Existing CCTV Systems | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 7 | Event Logging and Reporting | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 8 | Scalable AI Models | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 9 | Privacy Features (e.g., face blurring) | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | **✘** |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 10 | Offline Mode | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | **✘** |  |  | | --- | |  | | |  | | --- | | **✘** |  |  | | --- | |  | | |  | | --- | | **✘** |  |  | | --- | |  | |
| 11 | Crowd Behavior Analysis | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 12 | Object Tracking | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 13 | Anomaly Classification (e.g., aggression) | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |
| 14 | Multi-Camera Scalability | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | | |  | | --- | | ✔ |  |  | | --- | |  | |

**Architecture Diagram**



**References:**

* **Computer Vision and Video Analysis**
  + Redmon, J., & Farhadi, A. (2018). "YOLOv3: An Incremental Improvement."
  + Simonyan, K., & Zisserman, A. (2014). "Two-Stream Convolutional Networks for Action Recognition in Videos."
  + Sultani, W., Chen, C., & Shah, M. (2018). "Real-World Anomaly Detection in Surveillance Videos."
* **Anomaly Detection**
  + Chandola, V., Banerjee, A., & Kumar, V. (2009). "Anomaly Detection: A Survey."
  + Sabokrou, M., Fayyaz, M., Fathy, M., Moayed, Z., & Klette, R. (2017). "Deep-Anomaly: Fully Convolutional Neural Network for Fast Anomaly Detection in Crowded Scenes."