****

**SOP for Runway Surveillance System**

**Department of High Performance Computing (HPC)**

**Team Members**

Muhammad Affan Khan

Muhammad Rasib

Ahmed Hassan

**Supervision**

Mr. Abu Baker

Table Of Content

1. Introduction
2. Objective
3. Technologies Stack
4. System Demonstration
5. Use Case
6. Methodology
7. Future Work
8. Conclusion

01. Introduction

This project aims to revolutionize surveillance and security by automating the detection of anomalies in critical areas. By combining **computer vision**, **machine learning**, and **real-time processing**, it provides a robust solution for enhancing safety, reducing operational costs, and improving response times. The system is not only a technological advancement but also a practical tool for addressing real-world security challenges.

**1.1 Purpose**

**Objective of the Project:** The primary purpose of this project is to develop a **real-time computer vision system** capable of monitoring a **Region of Interest (ROI)** and detecting any unauthorized or anomalous entries. The system is designed to enhance security and operational safety in critical environments, such as airport runways, industrial facilities, or restricted zones.

**Core Functionality:**

* **Monitoring:** The system continuously observes the ROI using video feeds from surveillance cameras.
* **Anomaly Detection:** It employs advanced algorithms to identify objects, individuals, or activities that deviate from predefined norms or expected patterns.
* **Alert Generation:** Upon detecting an anomaly, the system triggers immediate alerts to notify security personnel or automated response systems.

**Applications:**

* **Airport Runways:** Detecting unauthorized vehicles, animals, or individuals on the runway to prevent accidents and ensure smooth operations.
* **Industrial Facilities:** Monitoring restricted areas to prevent unauthorized access and potential safety hazards.
* **Public Spaces:** Enhancing security in high-risk areas like government buildings, military bases, or event venues.

**Technological Focus:** The project leverages **computer vision**, **machine learning**, and **GPU-accelerated computing** to achieve high accuracy and low latency in anomaly detection. The use of **NVIDIA CUDA** and deep learning frameworks ensures efficient processing of video feeds, enabling real-time analysis and response.

**1.2 Why Use This System?**

**Addressing Critical Security Gaps:** Traditional surveillance systems often rely on human operators, who may experience fatigue or miss subtle anomalies. Automated systems like this one provide **24/7 monitoring** without human limitations, reducing the risk of oversight.

**Advantages Over Conventional Methods:**

* **Real-Time Detection:** Unlike manual monitoring, this system processes video feeds in real-time, ensuring immediate response to potential threats.
* **High Accuracy:** Machine learning models trained on relevant datasets can distinguish between normal and anomalous activities with high precision, minimizing false alarms.
* **Scalability:** The system can be deployed across multiple ROIs simultaneously, making it suitable for large or complex environments.
* **Integration with Existing Infrastructure:** It can be seamlessly integrated with existing security systems, such as access control or alarm systems, to create a comprehensive security solution.

**Operational Efficiency:**

* Reduces the need for constant human supervision, allowing security personnel to focus on strategic decision-making.
* Provides **audit trails** and **data logs** for post-event analysis, which can be crucial for investigations or compliance reporting.

**Cost-Effectiveness:** While the initial setup may require investment in hardware (e.g., GPUs) and software, the long-term benefits include reduced labor costs, fewer security breaches, and improved operational efficiency.

**1.3 Key Points**

**Technical Foundations:**

* **Computer Vision:** Uses algorithms to analyse video feeds and identify objects or activities within the ROI.
* **Region of Interest (ROI):** A user-defined area within the video feed where the system focuses its detection efforts. This allows for targeted monitoring and reduces computational overhead.
* **Anomaly Detection Algorithms:** Employs techniques such as:
  + **Background Subtraction:** Identifies moving objects by comparing frames.
  + **Object Detection:** Uses models like YOLO (You Only Look Once) or Faster R-CNN to classify and track objects.
  + **Behavioural Analysis:** Detects unusual patterns, such as loitering or unexpected movement trajectories.
* **Real-Time Alerts:** Alerts are generated instantly when an anomaly is detected, enabling rapid response.

**Future-Proofing:**

* The system is designed to be **upgradable**, allowing for the integration of newer algorithms or hardware as technology evolves.
* Supports **edge computing**, enabling deployment in remote or low-connectivity environments.
* Users can define multiple ROIs and set custom rules for what constitutes an anomaly (e.g., size, speed, or type of object).

**User Interface:**

* Provides a **dashboard** (e.g., via index.html) for real-time monitoring, alert management, and system configuration.
* Offers **visualizations** of detected anomalies, including timestamps, object types, and locations.

02. Objectives

This project aims to deliver a **high-performance, real-time computer vision system** for anomaly detection in critical environments. By focusing on **robustness, accuracy, low latency, and seamless integration**, the system will enhance security, reduce operational costs, and provide actionable insights. The objectives are designed to address both technical and practical challenges, ensuring the system is **scalable, adaptable, and future-proof**.

Further,

1. **Develop a Robust Computer Vision System**
   * **Goal:** Create a system that can reliably monitor and analyse video feeds in real-time to detect anomalies within a user-defined Region of Interest (ROI).
   * **Scope:**
     + Capture and process video streams from surveillance cameras.
     + Define and dynamically adjust ROIs based on user requirements.
     + Support continuous, 24/7 operation with minimal downtime.
2. **Achieve Accurate Anomaly Detection**
   * **Goal:** Implement algorithms that can precisely distinguish between normal and anomalous activities or objects within the ROI.
   * **Scope:**
     + Use machine learning models (e.g., YOLO, Faster R-CNN, or custom CNN architectures) to classify objects and behaviours.
     + Incorporate feature extraction techniques to identify subtle or complex anomalies (e.g., unusual movement patterns, unauthorized objects).
3. **Establish a Real-Time Alerting Mechanism**
   * **Goal:** Design a system that generates immediate alerts when anomalies are detected, enabling rapid response.
   * **Scope:**
     + Integrate alerting mechanisms such as visual/audible alarms, SMS/email notifications, or API calls to security systems.
     + Ensure alerts include relevant details (e.g., timestamp, location, type of anomaly).
4. **Ensure Low Latency and High Accuracy**
   * **Goal:** Optimize the system to operate with minimal delay and maintain high detection accuracy.
   * **Scope:**
     + Leverage GPU acceleration (e.g., NVIDIA CUDA) to process video frames at high speeds.
     + Fine-tune algorithms to balance speed and accuracy, reducing false positives while maintaining real-time performance.

**Technical Goals**

1. **Hardware Optimization**
   * Utilize **NVIDIA GPUs** (e.g., RTX A4000) for parallel processing to handle high-resolution video feeds efficiently.
   * Optimize resource usage to ensure the system can scale across multiple cameras or ROIs without performance degradation.
2. **Algorithm Development**
   * Develop or adapt **computer vision algorithms** for anomaly detection, such as:
     + **Deep learning-based object detection** for classifying objects (e.g., vehicles, humans, animals).
     + **Behavioural analysis** to detect unusual activities (e.g., loitering, unexpected trajectories).
3. **System Integration**
   * Seamlessly integrate with existing security infrastructure (e.g., CCTV networks, access control systems).
   * Provide APIs or SDKs for customization and third-party integrations.
4. **User-Centric Design**
   * Develop an intuitive **dashboard** (e.g., index.html) for configuring ROIs, viewing live feeds, and managing alerts.
   * Enable users to define custom rules for anomalies (e.g., size, speed, or type of object).

**Performance Metrics**

|  |  |  |
| --- | --- | --- |
| **Metric** | **Target** | **Justification** |
| Detection Accuracy | ≥ 95% | Ensures reliable identification of anomalies with minimal false alarms. |
| Latency | ≤ 200 ms per frame | Guarantees real-time processing for immediate alert generation. |
| Frame Rate | ≥ 30 FPS | Maintains smooth video analysis and reduces motion blur. |
| False Positive Rate | ≤ 5% | Minimizes unnecessary alerts, reducing operator fatigue and improving trust. |
| Scalability | Support ≥ 10 cameras/ROIs | Ensures the system can handle large or complex environments. |

**Operational Benefits**

1. **Enhanced Security**
   * Provides **proactive threat detection**, reducing the risk of unauthorized access or safety incidents.
   * Enables **faster response times** through real-time alerts and automated notifications.
2. **Cost Efficiency**
   * Reduces reliance on manual monitoring, lowering labor costs and human error.
   * Extends the lifespan of existing surveillance infrastructure by adding intelligent analysis capabilities.
3. **Data-Driven Insights**
   * Logs and analyses anomaly data to identify patterns or recurring issues.
   * Generates reports for compliance, audits, or operational improvements.
4. **Adaptability**
   * Supports **customizable rules** for different environments (e.g., airports, factories, public spaces).
   * Allows for **continuous learning**, where the system improves over time with additional data.

**Future-Ready Objectives**

1. **Multi-Camera Fusion**
   * Integrate data from **additional cameras** (e.g., thermal cameras) to enhance detection capabilities.
2. **Privacy-Compliant Design**
   * Implement **anonymization techniques** to protect individual identities while monitoring public or sensitive areas.

**Key Challenges and Mitigations**

|  |  |
| --- | --- |
| **Challenge** | **Mitigation Strategy** |
| Environmental Variability | Use adaptive algorithms to handle changes in lighting, weather, or camera angles. |
| False Positives/Negatives | Combine multiple detection methods (e.g., motion + object classification) for validation. |
| Computational Load | Optimize algorithms for GPU acceleration and distribute processing across multiple devices. |
| User Adoption | Provide training and documentation to ensure smooth operation and configuration. |

03. Technology Stack

**3.1 Hardware**

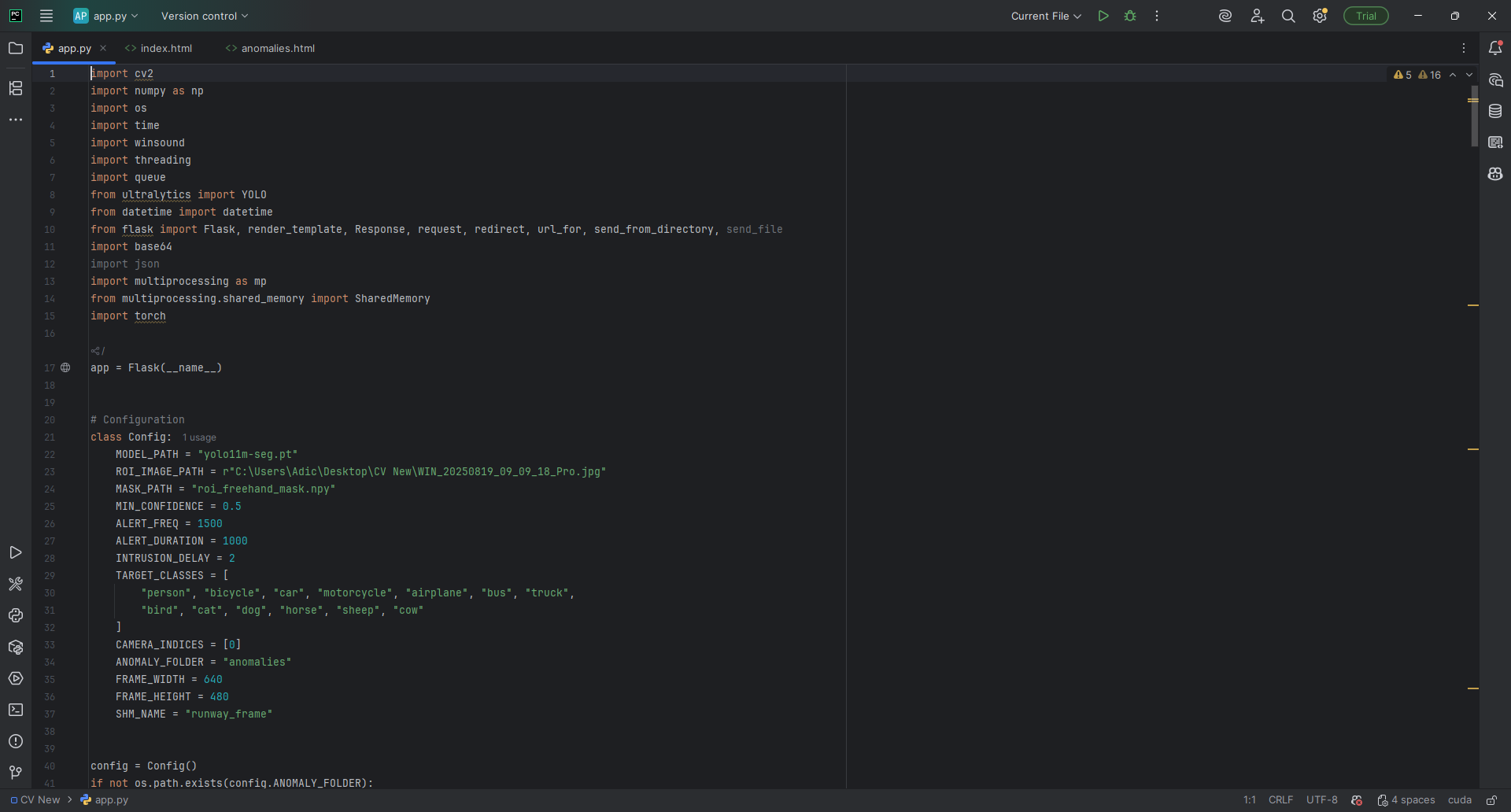
|  |  |  |
| --- | --- | --- |
| **Component** | **Details** | **Role in the Project** |
| GPU | NVIDIA RTX A4000, 16GB GDDR6, CUDA Cores, 140W TDP, Driver: 573.65, CUDA: 12.8 | Provides high-performance parallel processing for real-time video analysis, deep learning inference, and GPU-accelerated computing. |
| CPU | Intel Xeon Gold 6230R @ 2.10GHz, 26 Cores, 52 Threads, L3 Cache: 35.75MB, TDP: 150W | Handles general-purpose computing, multitasking, and manages system operations. Supports parallel processing for CPU-bound tasks. |
| RAM | 256GB DDR4 | Supports smooth multitasking, data processing, and handling large datasets or multiple video feeds simultaneously. |
| Storage | Total: 6TB (2TB SSD NVMe, 4TB HDD) | SSD: Fast read/write for OS, applications, and frequently accessed data. HDD: Cost-effective storage for logs, datasets, and backups. |
| Primary Storage (C:) | 2TB SSD NVMe (RAID 0), 1% Utilized (from Task Manager) | Hosts the OS, applications, and core project files for fast access. |
| Secondary Storage (E:) | 4TB HDD (RAID 0), 0% Utilized (from Task Manager) | Stores large datasets, video logs, and backups. |
| Cameras | Supports High-resolution IP cameras (e.g., 1080) | Captures video feeds for monitoring the ROI. |

**3.2 Core Software**

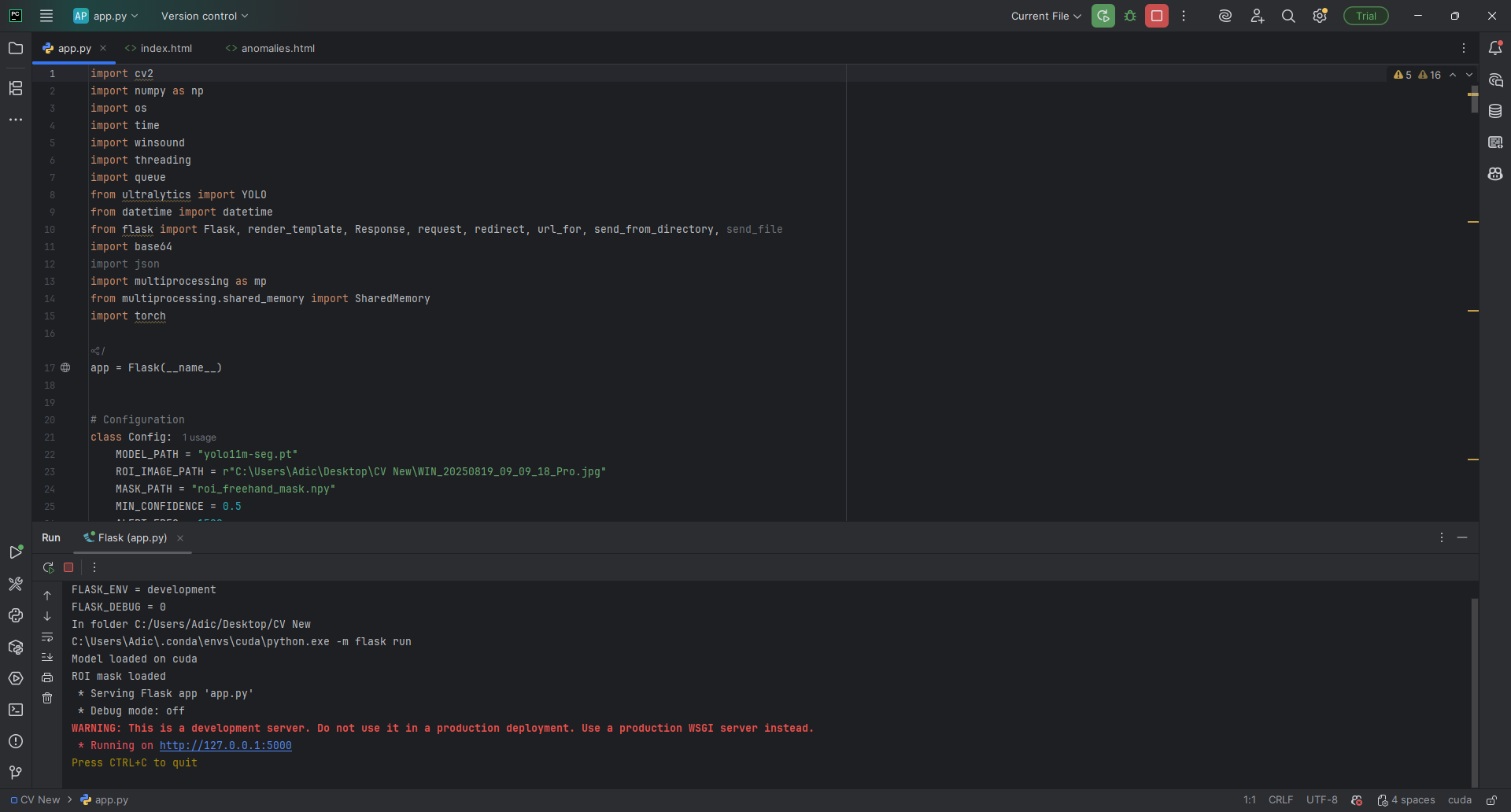
|  |  |  |
| --- | --- | --- |
| **Software** | **Version** | **Role in the Project** |
| CUDA Toolkit | 12.8 | Enables GPU-accelerated computing for tasks like image processing, model inference, and parallel computations. |
| cuDNN | 8.9.3 | Accelerates deep neural network operations (e.g., convolution, pooling) for faster training and inference. |
| NVIDIA Driver | 573.65 | Ensures compatibility and optimal performance between the GPU and software layers. |
| Python | 3.12 | Primary language for scripting, data processing, and integrating libraries (e.g., OpenCV, TensorFlow, PyTorch). |

04. System Demonstartation

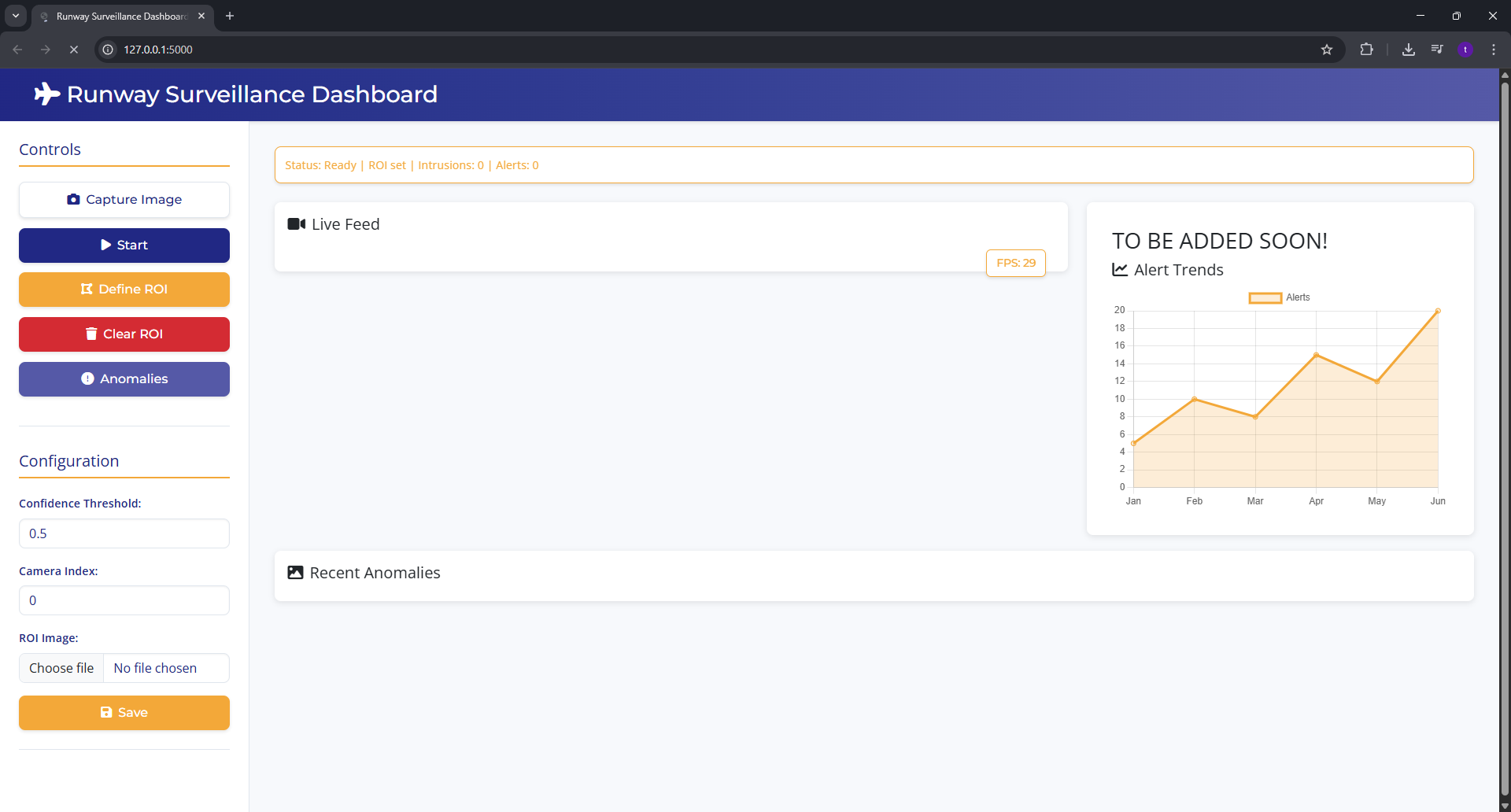
Initial startup View & the target classes to identify.

****

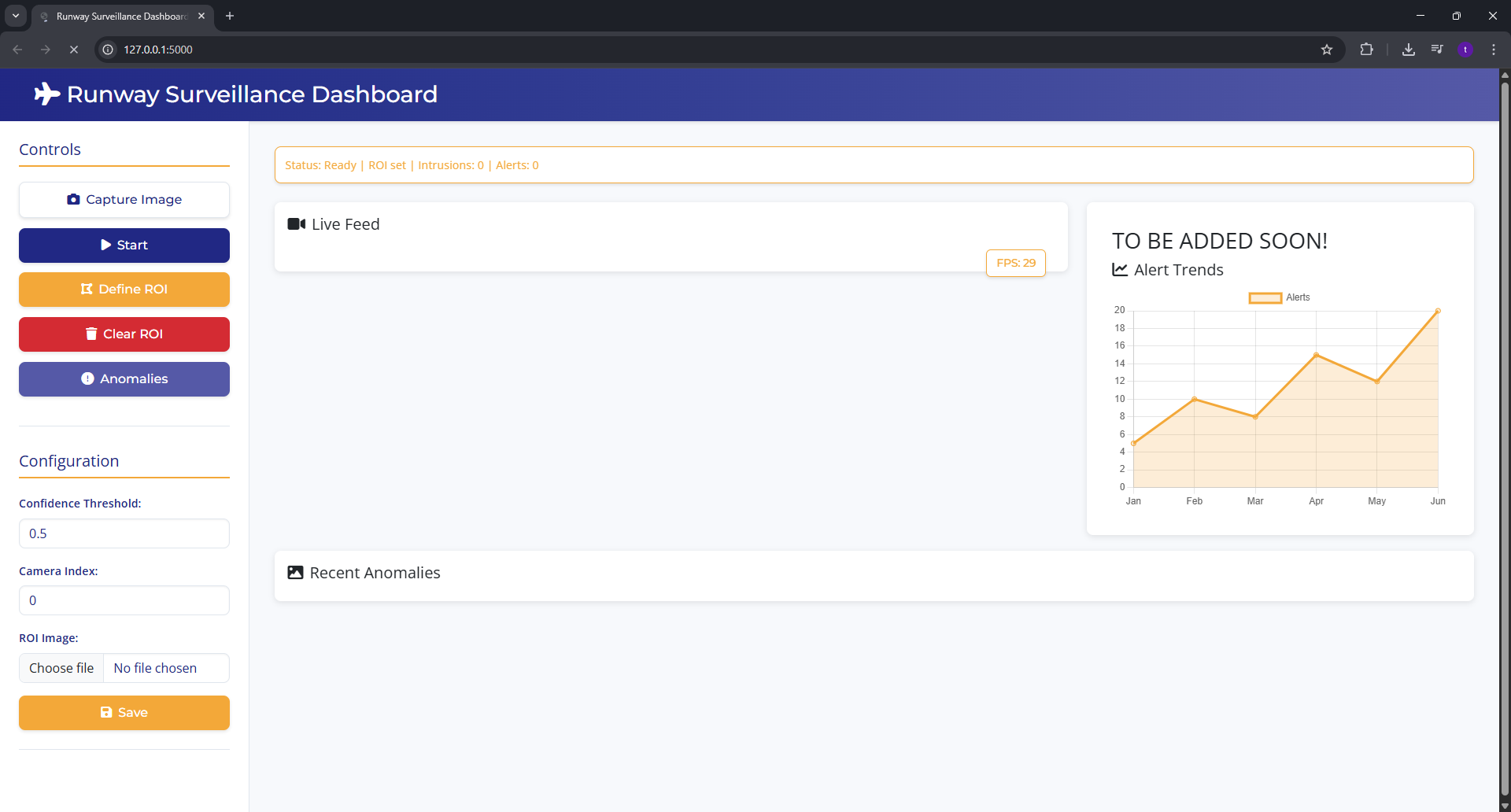
IP assigned to run the system.

****

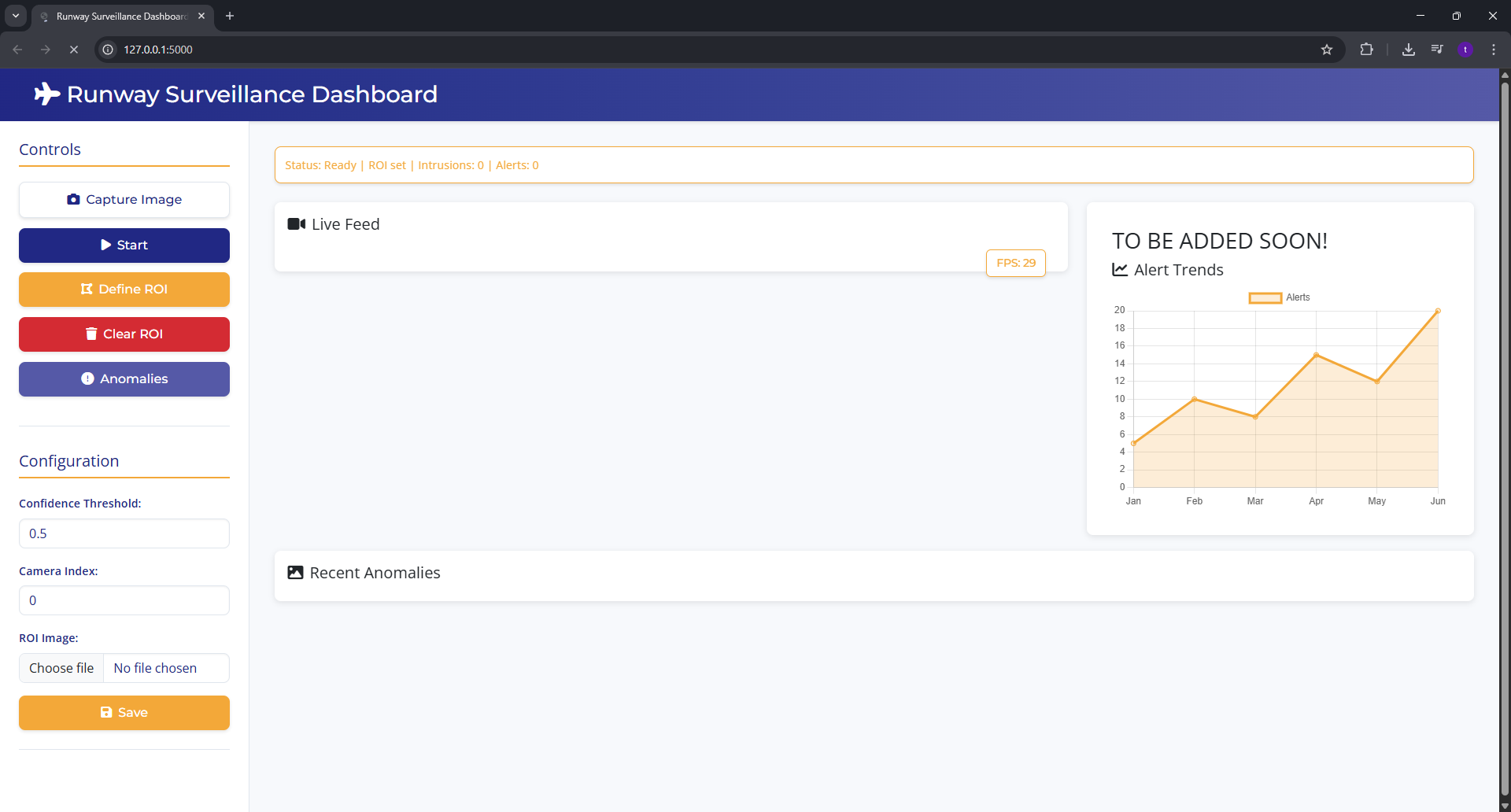
Main Page.

****

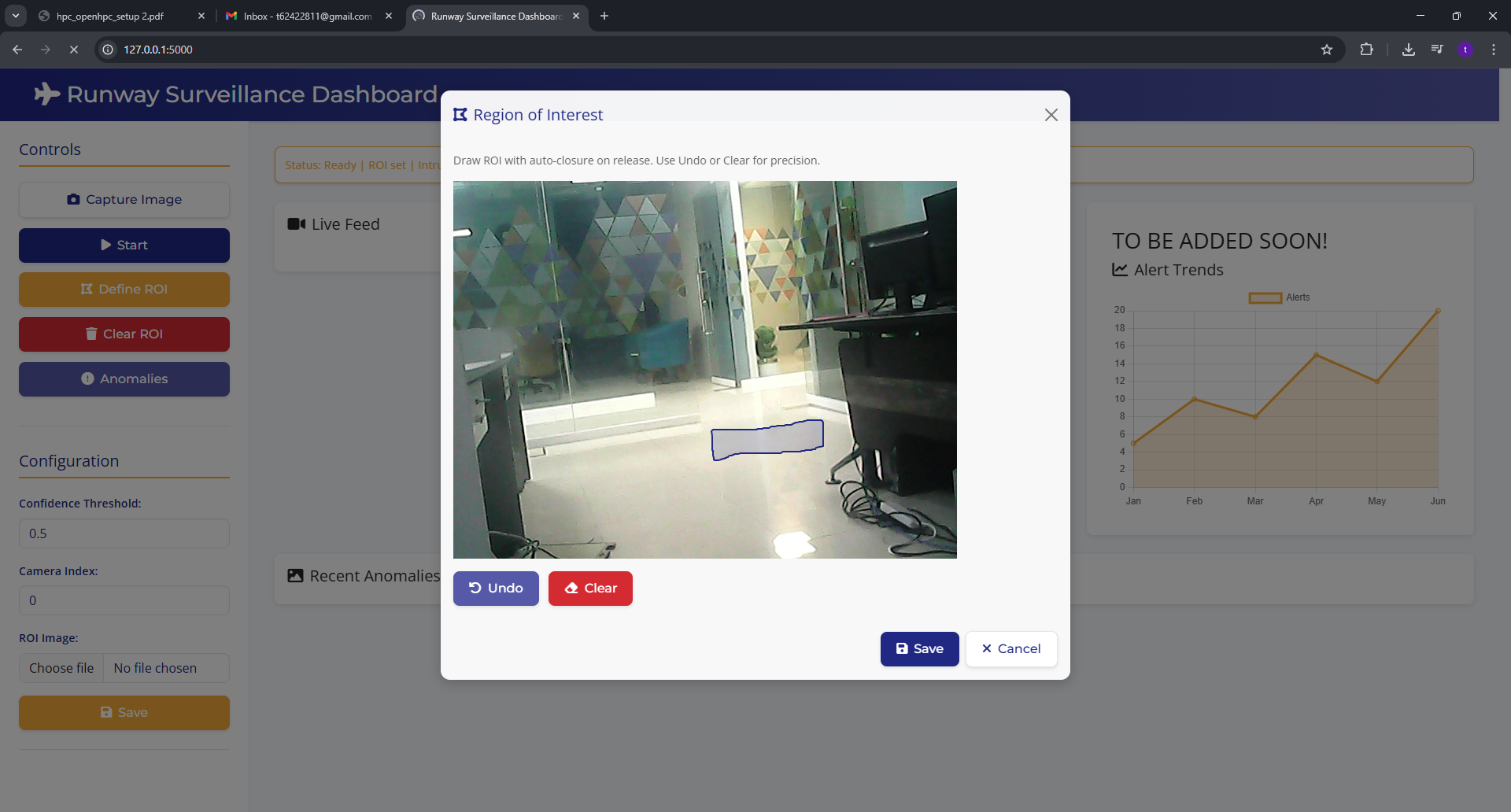
1. Can capture a live image or can also work on saved images
2. Threshold Values can also be changed at run time
3. Automatically detect the numbers of cameras, starting with the first detected camera (named as ‘0’ index)

****

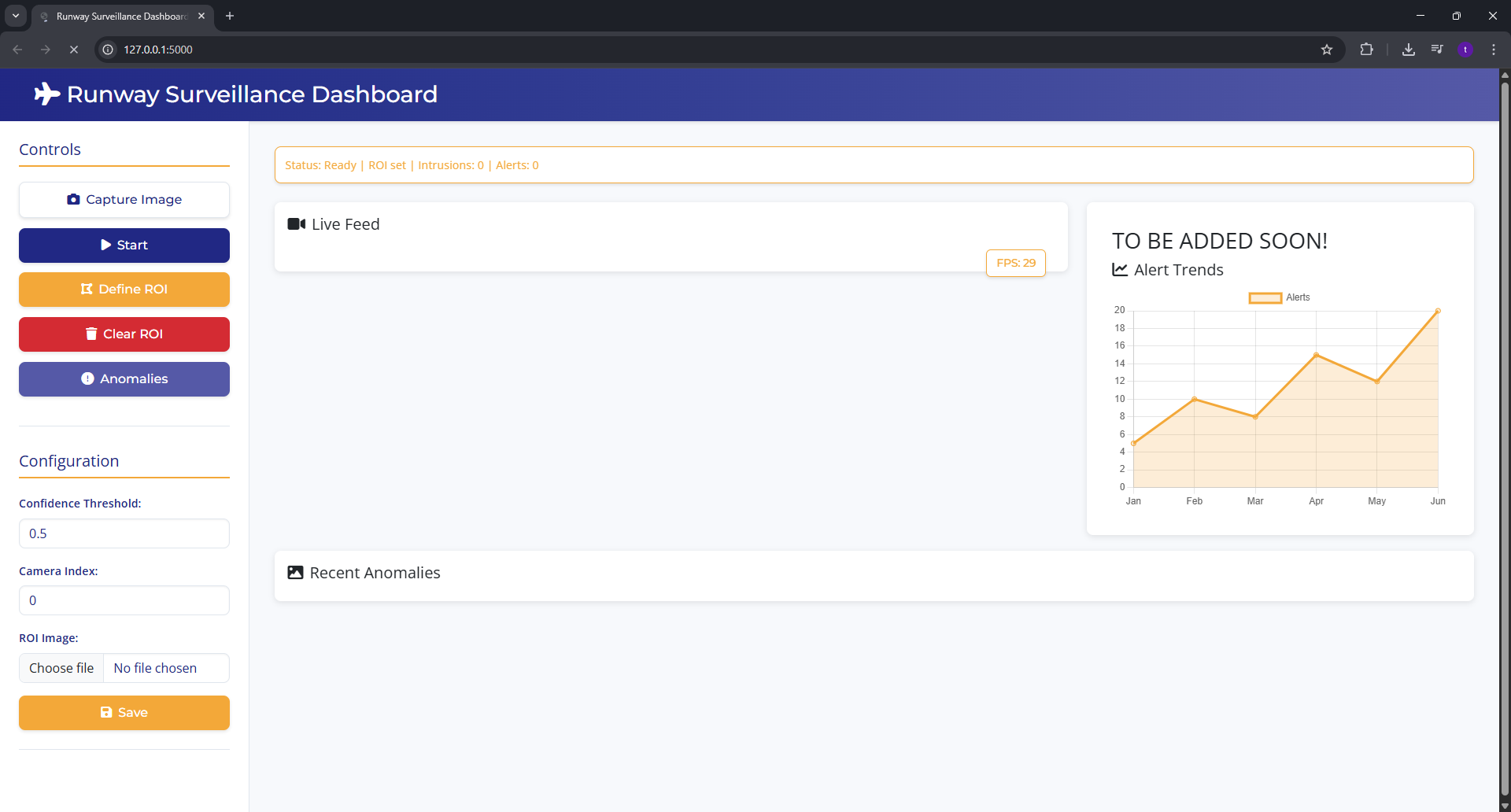
Draw ROI to begin the system (follows the live capture image process).

****

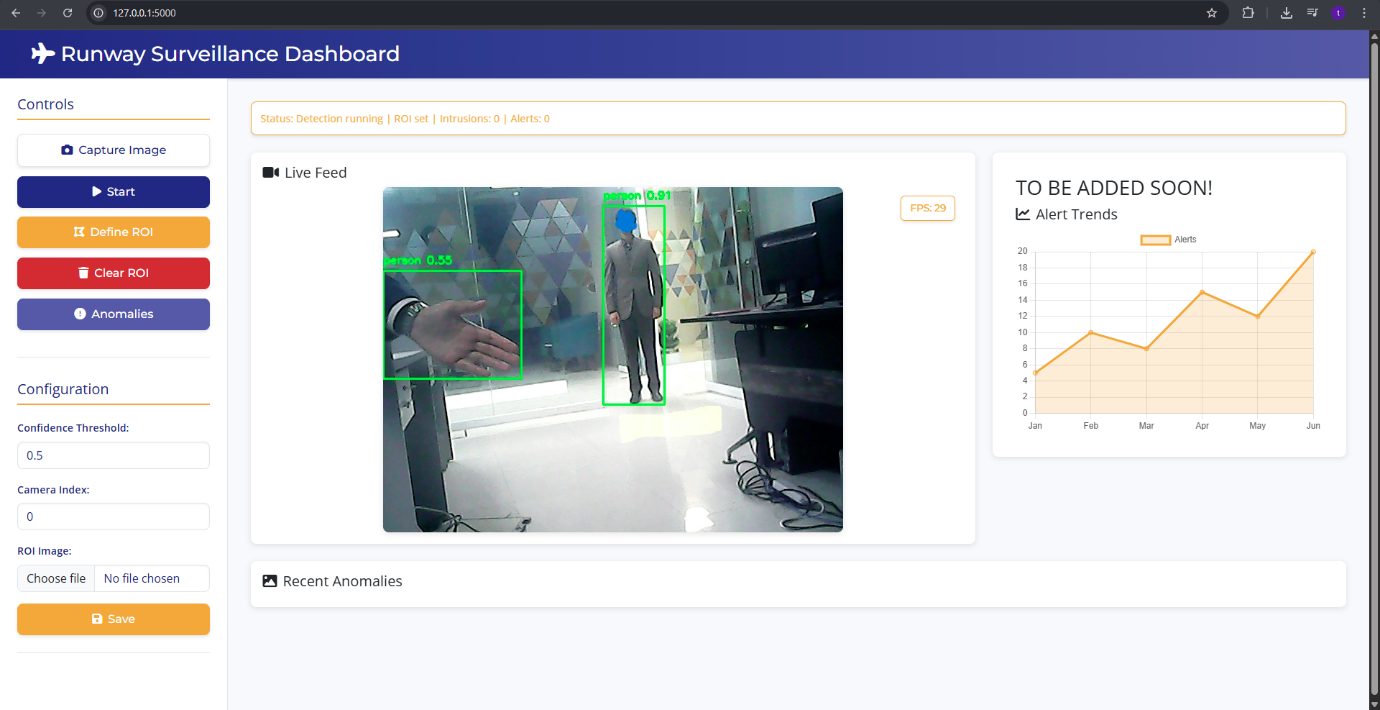
After drawing, you can save, undo to go back to the previous stage or even clear to start drawing again.

****

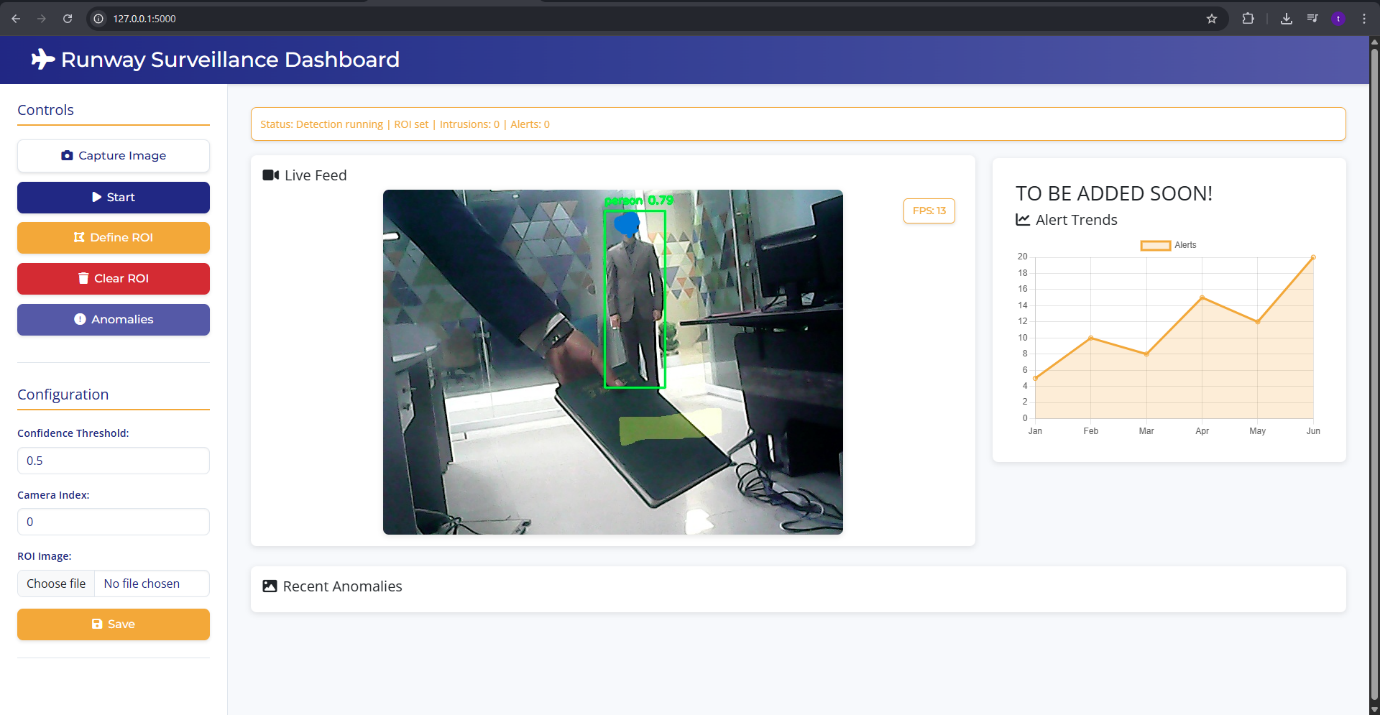
Click on Start to begin the surveillance.

****

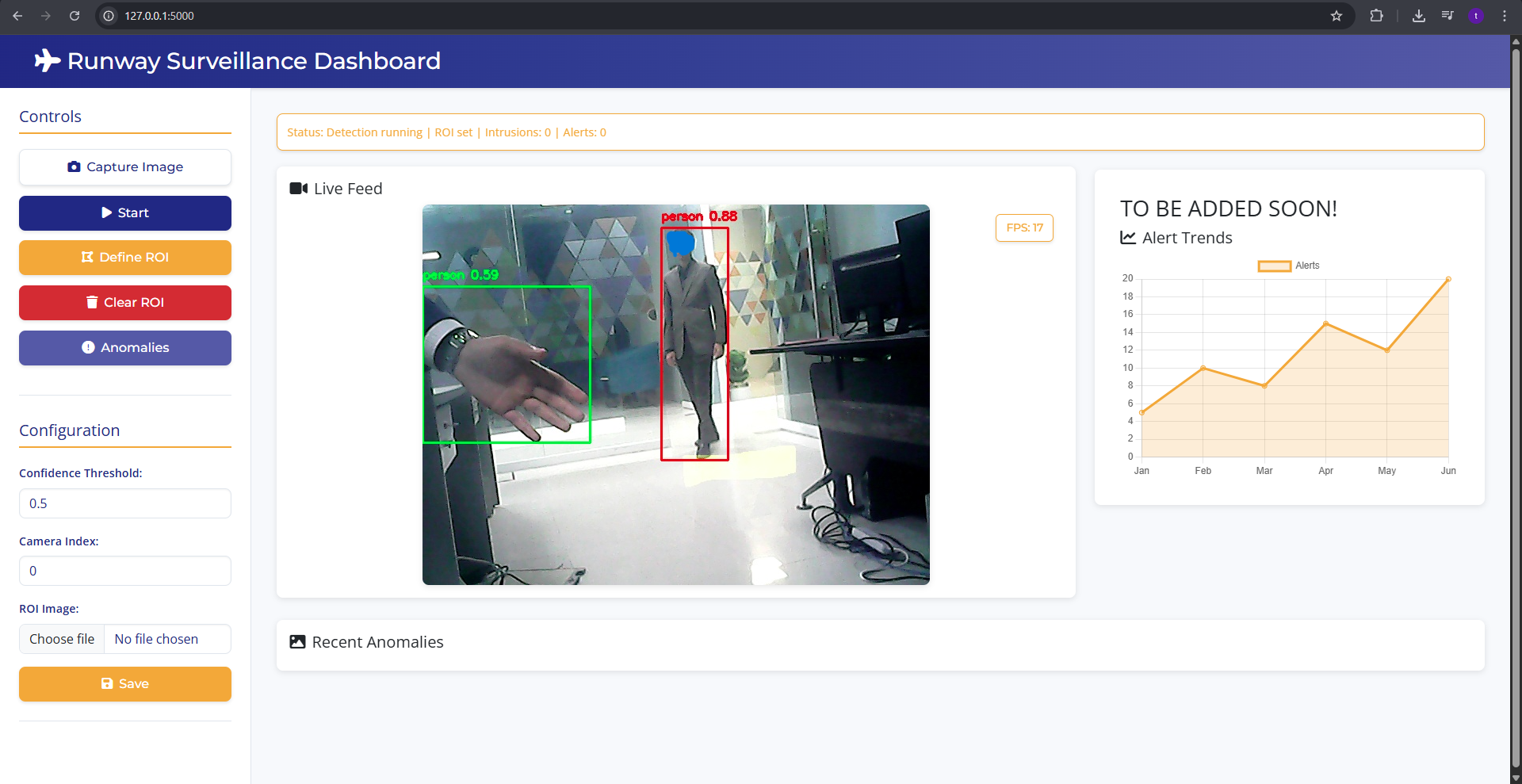
Safe Zone.

****

Save zone, even when a book is in ROI.

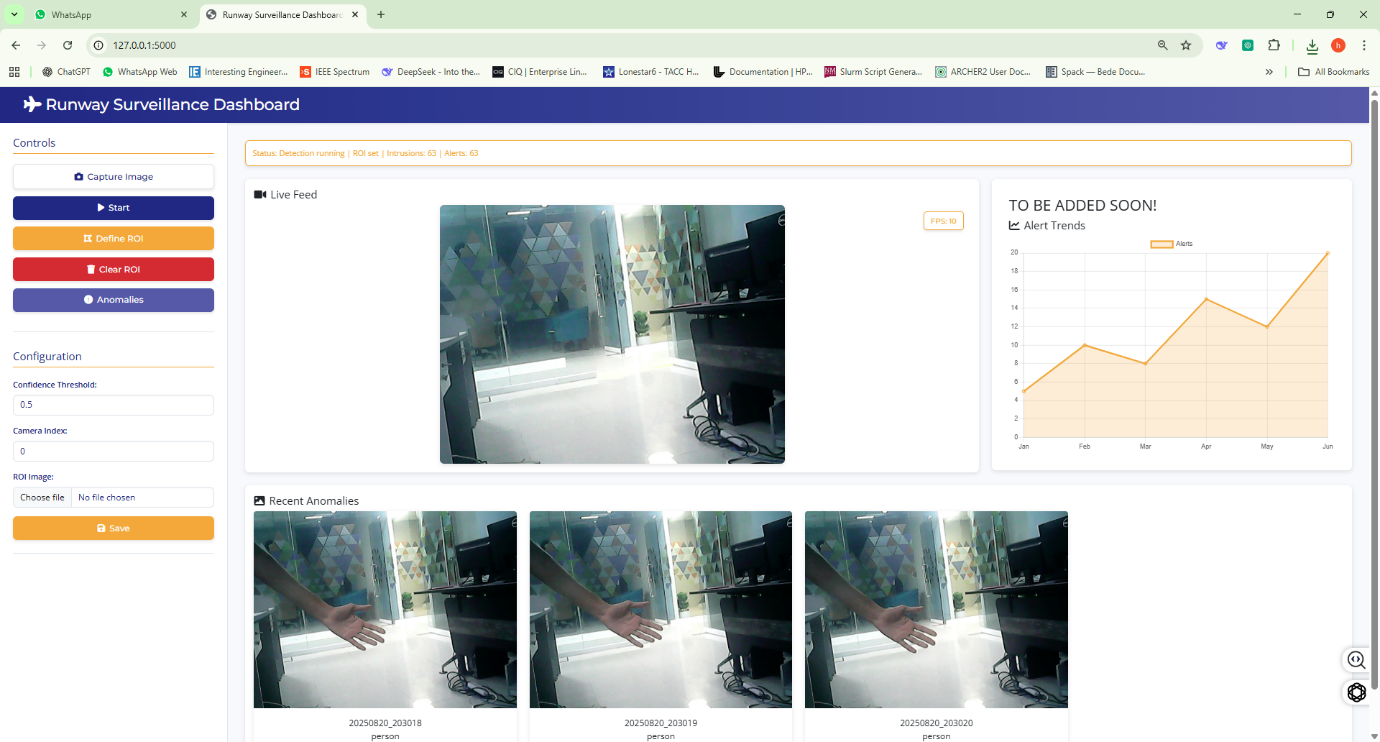
****

Alert generated when anomaly bypasses the parameter fencing.



****

Anomalies(Can be seen in two separate places.)

****

05. Use Case

**Runway intrusion detection system** leverages **computer vision, deep learning, and real-time alerting** to enhance **aviation safety and security**. By defining **critical ROIs**, detecting intrusions, and integrating with **airport security systems**, the system provides a **proactive, scalable, and compliant** solution for preventing unauthorized access to runways. The combination of **GPU acceleration, customizable alerts, and automated responses** ensures **rapid, accurate, and actionable** intrusion management.

**System Workflow**

**1. ROI Definition and Configuration**

* **Action:** Security personnel or system administrators define **multiple ROIs** around the runway using the system’s dashboard (index.html).
* **Tools Used:**
  + **OpenCV** for ROI selection and visualization.
* **Flexibility:**
  + ROIs can be **adjusted dynamically** (e.g., during maintenance or special events).
  + Different ROIs can have **custom sensitivity levels** (e.g., high alert for runway strips, medium for taxiways).

**2. Real-Time Video Capture and Processing**

* **Action:** IP cameras (1080p) stream live footage to the system.
* **Tools Used:**
  + **FFmpeg** for video stream decoding.
  + **OpenCV + CUDA** for real-time frame processing.
* **Performance:**
  + **≥ 30 FPS** processing to ensure smooth detection.
  + **GPU acceleration** (NVIDIA RTX A4000) for low-latency analysis.

**3. Anomaly Detection**

* **Action:** The system analyses each frame to detect objects or movements within and beyond the ROI.
* **Techniques Used:**
  + **Background Subtraction:** Identifies moving objects by comparing frames.
  + **Object Detection:** Uses **YOLO** (TensorFlow/PyTorch) to classify intruders (e.g., animal, person, vehicle).
* **Example:**
  + A Horse enters the runway strip → System classifies it as an "animal intrusion."
  + A person climbs the perimeter fence → System classifies it as a "person intrusion."

**4. Alert Generation**

* **Action:** Upon detecting an intrusion, the system generates an **immediate alert**.
* **Alert Types:**
  + **Visual Alerts:** Highlighted ROI on the dashboard with a bounding box around the intruder.
  + **Audible Alarms:** Sirens or pre-recorded alerts type at the control security posts.

**5. Response Coordination**

* **Action:** Security personnel receive the alert and take action.
* **Escalation Protocol:**
  + **Level 1:** Notification to on-duty security.
  + **Level 2:** Alert to airport operations and air traffic control (ATC).

**6. Logging and Reporting**

* **Action:** The system logs the event for post-incident analysis.
* **Data Stored:**
  + Type of intruder, response date & time.
  + Screenshot of the incident for review.

06. Methodology

The methodology outlines the **step-by-step process** the system follows to detect anomalies in the ROI and generate alerts. It ensures **real-time monitoring, accurate detection, and actionable reporting**.

**Step-by-Step Process**

**1. Video Capture**

* **Action:** The system captures **live video feeds** from cameras monitoring the predefined **Region of Interest (ROI)**.
* **Tools/Technologies:**
  + IP cameras (1080p/4K resolution).
  + **OpenCV** for video stream acquisition.
* **Output:** Continuous video feed for real-time analysis.

**2. Anomaly Detection**

* **Action:** The system analyzes the video feed to detect anomalies using **pre-trained models or algorithms**.
* **Approach:**
  + **Pre-trained Models:** Utilizes models (e.g., YOLO) trained on relevant datasets to classify objects or behaviors.
  + **Predefined Criteria:** Detects anomalies based on rules such as unauthorized objects, unexpected movement, or specific patterns.
* **Output:** Identified anomalies (e.g., intruders, unauthorized vehicles) within the ROI.

**3. Alert Generation**

* **Action:** Upon detecting an anomaly, the system generates an **immediate alert**.
* **Alert Types:**
  + **Visual Alerts:** Highlights the anomaly on the dashboard (e.g., bounding box, ROI emphasis).
  + **Audible Alarms:** Triggers sirens or alerts in the control room.
  + **Notifications:** Sends alerts to security personnel via **SMS, email, or push notifications**.
* **Output:** Real-time alerts for rapid response.

**4. Logging and Reporting**

* **Action:** The system **logs all detected anomalies** and actions taken.
* **Data Recorded:**
  + Timestamp of the anomaly.
  + Type of anomaly (e.g., intruder, vehicle).
  + Location (ROI coordinates).
  + Response actions (e.g., alert sent, alarm triggered).
* **Output:** Structured logs for **analysis, auditing, and reporting**.

07. Future Work  
  
The future development of this system can be within the **military domain** aims to significantly expand its capabilities to meet the demands of modern defence operations. Currently, the system provides a robust foundation for real-time anomaly detection in a defined Region of Interest (ROI). Moving forward, the focus will be on enhancing its applications for **surveillance and threat detection**. This includes deploying the system to monitor military bases, borders, and restricted zones, ensuring 24/7 surveillance even in harsh environments using thermal and low-light cameras. Additionally, the system will be adapted to detect and neutralize hostile drones by integrating radar and RF sensors, along with developing automated countermeasures like signal jamming and intercept drones.

Another key area of development is the integration of the system into **autonomous military systems**. This involves embedding the technology into unmanned ground vehicles (UGVs) for reconnaissance missions in high-risk areas, enabling real-time obstacle and threat detection for improved navigation. The system will also be integrated with autonomous weapon systems, ensuring precision engagement while maintaining human-in-the-loop oversight to adhere to ethical standards.

To further bolster its effectiveness, the system will incorporate **cyber-physical security** features. This includes combining the system with cybersecurity measures to detect and respond to both physical and digital threats. Secure communication protocols and tamper-proof logging using blockchain technology will ensure data integrity and prevent unauthorized access or tampering.

Enhancements in **advanced detection capabilities** are also planned. By combining multiple sensors such as LiDAR, radar, and thermal imaging, the system will achieve improved detection accuracy even in challenging conditions like smoke or fog. AI-driven models will be developed to fuse data from these sensors, reducing false positives and enhancing overall reliability. Predictive analytics will be employed to anticipate potential threats based on historical data and behaviour patterns.

Finally, the system will be integrated with **existing military infrastructure**, such as C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) systems, to provide real-time situational awareness to command centres. Automated response systems will be implemented to trigger defences like barriers, alarms, and countermeasures upon detecting threats, ensuring rapid and coordinated responses. These advancements will transform the system into a critical component of modern defence systems, enhancing security, autonomy, and response capabilities.

08. Conclusion

This project successfully implements a **real-time runway surveillance system** using **computer vision and deep learning** to detect and alert anomalies within a defined Region of Interest (ROI). The system leverages **YOLOv11 for segmentation**, **OpenCV for video processing**, and **Flask for a user-friendly dashboard**, ensuring robust performance and ease of use. By capturing live video feeds, analysing them for unauthorized intrusions (such as people, animals, or vehicles), and generating **visual, audible, and notification-based alerts**, the system enhances security and operational safety in critical environments like airport runways.

The **modular architecture** allows for **customizable ROI selection**, **adjustable confidence thresholds**, and **multi-camera support**, making it adaptable to various use cases. The integration of **shared memory for efficient frame processing** and **multiprocessing for parallel tasks** ensures **low-latency performance**, while the **logging and screenshot capture** features provide a comprehensive record of detected anomalies for further analysis.

The **web-based dashboard** offers an intuitive interface for monitoring, configuring, and reviewing anomalies, with features like **real-time video feeds**, **ROI definition tools**, and **anomaly logs**. The system’s design prioritizes **scalability, accuracy, and reliability**, making it a valuable tool for **aviation security, perimeter monitoring, and intrusion detection**.

Future enhancements could include **multi-sensor fusion** (e.g., thermal cameras, LiDAR), **AI-driven predictive analytics**, and **integration with broader security systems** (e.g., access control, automated response mechanisms). This project not only addresses immediate security challenges but also lays the groundwork for **smarter, more autonomous surveillance systems** in the future. With its **open architecture and extensible design**, the system can be further developed for applications in **military surveillance, industrial safety, and smart city monitoring**.