A Minor Project

Report on

AI-Powered Suspicious Activity Detection System Using Computer Vision

By

Sakshi Patel - 21BIT163
Prerana Somani - 21BIT180
Sakhi Patel - 21BIT182

Under the Guidance of

Dr. Paawan Sharma

Associate Professor

Submitted to

The Department of Information and Communication Technology,

School of Technology,

Pandit Deendayal Energy University, Gandhinagar

AY 2024-2025

CERTIFICATE

This is to certify that the seminar report entitled "**AI-Powered Suspicious Activity Detection System Using Computer Vision**" submitted by **Sakshi Patel (21BIT163), Prerana Somani (21BIT180)** and **Sakhi Patel(21BIT182)** has been conducted under the supervision of **Dr. Paawan Sharma, Associate Professor, Department of ICT**, and is hereby approved for the partial fulfilment of the requirements for the award of the degree of Bachelor of Engineering in the Department of **Information and Communication Technology Engineering** at Pandit Deendayal Energy University, Gandhinagar. This work is original and has not been submitted to any other institution for the award of any degree.

Sign:

Name of Guide: Dr. Paawan Sharma
Designation: Associate Professor
Department: Department of ICT

School of Technology,

Pandit Deendayal Energy University, Gandhinagar

Sign:

Name of Examiner:

Designation:

Department:

School of Technology,

Pandit Deendayal Energy University, Gandhinagar

DECLARATION

We hereby declare that the minor project report entitled "AI-Powered Suspicious Activity Detection System Using Computer Vision" is the result of my/our own work and has been written by me. This report has not utilized any language model or natural language processing artificial intelligence tools for the creation or generation of content, including the literature survey.

The use of any such artificial intelligence-based tools was strictly confined to the polishing of content, spell checking, and grammar correction after the initial draft of the report was completed. No part of this report has been directly sourced from the output of such tools for the final submission.

This declaration is to affirm that the work presented in this report is genuinely conducted by me and to the best of my knowledge, it is original.

Sakshi Patel - 21BIT163

Prerana Somani - 21BIT180

Sakhi Patel - 21BIT182

Information and Communication Technology Department,

School of Technology,

Pandit Deendayal Energy University,

Gandhinagar

Date:10-12-2024

Place:

ACKNOWLEDGEMENT

We would like to express our heartfelt gratitude to **Dr. Paawan Sharma**, Associate Professor, Department of Information and Communication Technology, Pandit Deendayal Energy University, Gandhinagar, for his invaluable guidance, constant encouragement, and support throughout the completion of our minor project titled *"AI-Powered Suspicious Activity Detection System Using Computer Vision."* His insightful feedback and expertise were pivotal in shaping the direction of this project.

We also extend our gratitude to the **Department of Information and Communication Technology, School of Technology, Pandit Deendayal Energy University**, for providing us with the necessary resources and a conducive environment to undertake this project.

We are immensely thankful to our peers, family, and friends, whose unwavering support and motivation inspired us to persevere and successfully complete this endeavor.

Lastly, we would like to acknowledge the contributions of the open-source community and platforms such as Kaggle for providing valuable datasets that were instrumental in the execution of this project.

Sincerely,
Sakshi Patel (21BIT163)
Prerana Somani (21BIT180)
Sakhi Patel (21BIT182)

LIST OF FIGURES

LIST OF TABLES

TABLE OF CONTENTS

Introduction and Objectives

Introduction

Public spaces such as malls, parks, and transportation hubs are increasingly vulnerable to safety threats posed by suspicious activities. Traditional surveillance systems often depend on human operators to keep an eye on numerous camera feeds. This approach can be challenging, as it's easy for people to become overwhelmed, tired, or distracted, leading to slower responses and occasional errors.

To address these challenges, the proposed **AI-Powered Suspicious Activity Detection System Using Computer Vision** leverages advancements in artificial intelligence and machine learning to enhance public safety. By integrating computer vision techniques with real-time video analysis, the system aims to automatically detect and flag suspicious activities. This proactive approach empowers security personnel to respond swiftly and effectively to potential threats, minimizing risks and ensuring safer public environments.

Objectives

1. **Develop an automated detection system**
    - Employ cutting-edge computer vision algorithms to analyze surveillance footage and identify activities categorized as suspicious.
2. **Enable real-time monitoring**
    - Implement real-time video processing to detect and alert security teams immediately upon identifying suspicious behavior.
3. **Enhance detection accuracy**
    - Train and optimize machine learning models to minimize false positives and false negatives, ensuring high reliability in varied environments.
4. **Provide intuitive alerts**
    - Design a notification mechanism (e.g., SMS, email, or dashboard alerts) for security personnel, ensuring timely responses to potential threats.
5. **Ensure scalability and adaptability**
    - Create a system architecture that is scalable for deployment across various public spaces and adaptable to evolving security requirements.

This project aims to revolutionize the traditional surveillance system by making it smarter, faster, and more reliable, contributing significantly to public safety and security management.

Literature Review

AI-Powered Suspicious Activity Detection System Using Computer Vision.

SR. NO.	ARTICLE TITLE	AUTHOR	YEAR	FINDINGS	LIMITATIONS
1	Suspicious Activity Detection in Surveillance Footage	Sathyajit Loganathan, Gayashan Kariyawasam, Prasanna Sumathipala	2019	The paper discusses a system for detecting suspicious activities in surveillance footage using advanced image processing and machine learning techniques.	The system's accuracy is reduced in low-light conditions and crowded environments. It also requires extensive training data to reduce false positives.
2	Smart Security System for Suspicious Activity Detection in Volatile Areas	Dr. Joy Iong Zong Chen	2020	Developed a smart security system using AI and image processing for real-time suspicious activity detection in high-risk areas.	Accuracy drops in poor lighting and weather. High computational power limits scalability and adaptability to new threats.
3	Camera Surveillance Using Raspberry Pi	Priya Meghana Raavi, Hiranmayee Panchangam	2020	Describes a low-cost surveillance system using Raspberry Pi for real-time monitoring and motion detection.	Limited by hardware capabilities, poor lighting, and an unstable internet. Suitable for small-scale use.

4	A Raspberry-Pi based Surveillance Camera with Dynamic Motion Tracking	Oussama Tahan	2020	This paper introduces a surveillance camera system powered by Raspberry Pi that can actively follow motion. It uses smart motion detection algorithms to track objects as they move.	The system faces challenges with its limited processing power, which can impact its ability to track objects in real time. Additionally, its motion detection struggles in low-light conditions and with complicated backgrounds, reducing its accuracy.
5	Suspicious Activity Detection from Videos using YOLOv3	Nipunjita Bordoloi, Anjan Kumar Talukdar, Kandarpa Kumar Sarma	2020	The paper demonstrates using YOLOv3 (You Only Look Once) for detecting suspicious activities in videos. YOLOv3 provides real-time object detection with high accuracy.	The model's performance can vary depending on the video resolution and lighting conditions. In crowded scenes or complex environments, it might overlook certain activities, which can result in missed detections or false negatives.s.
6	Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video	Esakky Selvi, Malaiyalathan Adimoolam, Govindharaju Karthi, Kandasamy Thinakaran, Nagaiah Mohanan Balamurugan, Raju Kannadasan, Chitapong Wechtaisong,	2022	Developed an enhanced CNN for detecting suspicious actions from surveillance videos with improved accuracy.	Limited by video quality, lighting conditions, and complexity in crowded scenes. Requires high computational power.

		Arfat Ahmad Khan			
7	Internet-of-Things-Based Suspicious Activity Recognition Using Multimodalities of Computer Vision for Smart City Security	Amjad Rehman, Tanzila Saba, Muhammad Zeeshan Khan, Robertas Damaševičius, Saeed Ali Bahaj	2022	The paper presents an IoT-based system using computer vision to detect suspicious activities in smart cities. It integrates multiple modalities for enhanced accuracy and real-time monitoring.	The system faces challenges with the real-time processing under poor network conditions. It also struggles with accurately identifying activities in crowded environments and varying lighting conditions.
8	Propounding First Artificial Intelligence Approach for Predicting Robbery Behavior Potential in an Indoor Security Camera	SHIMA POUYAN, MOSTAFA CHARMI, ALI AZARPEYVAND, HOSSEIN HASSANPOOR	2023	Proposes an AI-based system using indoor security cameras to predict potential robbery by analyzing human behavior and movement patterns.	Limited by data diversity, challenges with an occlusion (obstructed views), and high computational requirements for real-time processing. May result in false positives.
9	An Analysis of Artificial Intelligence Techniques in Surveillance Video Anomaly Detection: A Comprehensive Survey	Erkan Şengönül, Refik Samet, Qasem Abu Al-Haija, Ali Alqahtani, Badraddin Alturki, Abdulaziz A. Alsulami	2023	Surveys AI techniques for anomaly detection in surveillance videos, to emphasize machine learning and deep learning methods. Highlights the need for effective feature extraction and dataset diversity.	Many systems struggle with high false alarm rates and rely on large labeled datasets to function effectively. Their performance often fluctuates due to changing environmental conditions and the complexity of human behavior, making detection inconsistent at times.

10	Pattern Recognition Algorithm to Detect Suspicious Activities	V C Mahavishnu, S G Vikhas, T Shyamganesh ,S Roopakumar, S V Kavin	2023	Introduces a pattern recognition algorithm for detecting suspicious activities in surveillance videos, enhancing accuracy and response time.	The system's performance can be influenced by environmental factors, sometimes leading to false positives in more complicated situations. It also relies on a large amount of training data, which can be challenging to gather.

Research Gaps and Problem Statement

Research Gaps

1. **Reliance on manual surveillance**
    - Current surveillance systems rely on human operators to monitor multiple feeds simultaneously. This approach is prone to fatigue, distractions, and human error, reducing the effectiveness of detecting suspicious activities in real-time.
2. **Limited real-time detection capabilities**
    - Existing systems often lack the capability to process and analyze video feeds in real-time, leading to delayed responses during critical situations.
3. **A High rate of false alarms**
    - Many automated surveillance systems generate false positives due to poorly trained algorithms, causing unnecessary alerts and reducing trust in the system.
4. **Inadequate scalability**
    - Current solutions often fail to adapt to large-scale deployments in varied environments, such as malls, public transport hubs, and parks, with dynamic activity patterns.
5. **Lack of context-aware detection**
    - Existing models struggle to interpret the context of activities, which is essential to differentiate between normal and suspicious behavior.

Problem Statement

Public spaces face increasing safety risks due to suspicious activities, with traditional surveillance systems proving inefficient for real-time threat detection and response. Human monitoring of surveillance footage is prone to errors and delays, often resulting in missed or delayed identification of threats.

This project aims to bridge these gaps by developing an **AI-Powered Suspicious Activity Detection System Using Computer Vision**. The proposed solution will leverage advanced computer vision techniques and real-time video analysis to automatically detect and classify suspicious activities, providing timely alerts to security personnel for faster intervention.

This research tackles the shortcomings of current systems and proposes a smarter, more adaptable, and dependable solution to improve public safety with intelligent surveillance technology.

Methodology

The methodology for this project is divided into three main stages: **Dataset Preparation and Model Training**, **Inference and Detection**, and **Suspicious Activity Identification**. The steps are outlined below:

1. Dataset Preparation and Model Training

Objective: Train a YOLOv8 model to detect objects relevant to suspicious activities (e.g., weapons and persons).

Steps:

- **Data Annotation:**
  - Use tools like LabelImg or Roboflow (if needed) to annotate images for specific object categories, such as knife_weapon and person.
- **Preprocessing and Configuration:**
  - Prepare a dataset with well-labeled images and split it into training and validation subsets.
  - Create a YOLO configuration file (data.yaml) specifying classes and dataset paths.
- **Transfer Learning:**
  - Load a pre-trained YOLOv8 model (yolov8n.pt).
  - Locking the initial layers allows the system to make use of general features, while fine-tuning the later layers helps it focus on specific detection tasks.
- **Training the Model:**
  - Adjust training parameters such as the number of epochs, image size, the batch size, confidence threshold, and IoU threshold to optimize performance.
  - Train the model with the prepared dataset.
  - Save the fine-tuned model (my_yolov8_model.pt).

2. Inference and Detection

Objective: Use the trained YOLOv8 model for real-time or video-based object detection.

Steps:

- **Model Loading:**
  - Load the fine-tuned “YOLOv8” model for inference.
- **Video Stream Input:**
  - Capture video frames using OpenCV, either from a file or webcam.

- **Object Detection:**
    - Perform inference on each frame to detect objects such as knives and persons.
    - Access detected bounding boxes, confidence scores, and class IDs from the model's output.
- **Visualization:**
    - Render detection results on video frames, highlighting detected objects and labeling them appropriately.

3. Suspicious Activity Identification

Objective: Analyze detection results to identify and flag suspicious activities.

Steps:

- **Activity Rules:**
    - Define rules for identifying suspicious activity, e.g., a knife near a person indicates a potential threat.
    - Calculate the Euclidean distance between detected objects' bounding box centers to determine proximity.
- **Real-Time Detection:**
    - Continuously monitor frames for suspicious activities and flag alerts.
- **Labeling and Notification:**
    - Mark objects of interest as "Suspicious" on the video frames.
    - Implement optional notifications or logging for flagged events.
- **Optimization:**
    - Fine-tune thresholds (e.g., proximity distance) and parameters for detection confidence to minimize false positives and false negatives.

Details of Work Execution

1. Data Preparation

The foundation of this project lies in training an accurate detection model. This stage involved:

- **Dataset Acquisition**: A labeled dataset was sourced from Kaggle, containing images of suspicious objects (e.g., knives, weapons) and human activities.
- **Data Augmentation**: Techniques like rotation, scaling, and flipping were applied to enhance the model generalization.
- **Configuration**: A YAML file was created to set up the training for YOLOv8, detailing the dataset paths, classes, and other key configurations.

2. Model Training

The model was trained using the following steps:

- **Load Pre-trained Model**: The YOLOv8 model (yolov8n.pt) was loaded as a base model.
- **Layer Freezing**: To transfer knowledge from the pre-trained model, the first 100 layers were frozen, reducing training complexity and computational cost.
- **Custom Training**: The model was trained on the custom dataset using parameters like:
  - **Image Size**: 320 pixels for computational efficiency
  - **Batch Size**: 8 for memory optimization
  - **Confidence Threshold**: 0.25 to filter the weak detections
  - **IoU Threshold**: 0.5 for Non-Max Suppression.
- **Model Saving**: The YOLOv8 model was trained and saved as my_yolov8_model.pt, ready to be used for making predictions.

3. Real-Time Suspicious Activity Detection

Code Implementation for Detection

1. **Loading the Model**:
   The trained YOLOv8 model was loaded to make predictions.
2. **Video Stream Input**:
   Video feeds from local files or live webcams were processed.
3. **Detection of Objects and Activities**:
   The model was used to detect objects like knives (class ID 0) and people (class ID 1) in the frames.
   - **Detection Results**: Bounding boxes, confidence scores, and class IDs were extracted.

4. **Suspicious Activity Logic**:
   - A function nearby_person() was implemented to detect proximity between a knife and a person.
   - If proximity was below the defined threshold (50 pixels), the activity was flagged as suspicious, triggering an alert in the console.
5. **Visualization**:
   Detected objects were labeled as "Suspicious" and displayed with bounding boxes on the video frame for better interpretability.

4. Alert System

A real-time notification system was integrated, allowing security personnel to be promptly informed when suspicious activity was detected.

5. Testing and Validation

The system's performance was evaluated using:

- **Precision and Recall Metrics**: To measure the accuracy and sensitivity of detection.
- **Real-World Scenarios**: Video streams of staged suspicious activities were tested to validate real-time detection capabilities.

6. Deployment and Scalability

The system was built to adapt to different environments by training the model using a variety of datasets.

- Training the model with a variety of datasets.
- Ensuring compatibility with multiple camera systems and cloud platforms for large-scale deployment.

Results and Discussions

1. Performance Metrics

The trained YOLOv8 model was evaluated using key metrics, highlighting its effectiveness in detecting suspicious activities:

- **Precision**: The model achieved a precision score of 0.87, indicating a high accuracy in correctly identifying suspicious objects and activities.
- **Recall**: A recall score of 0.83 demonstrated the model's ability to detect most true positive instances of suspicious activity.
- **Mean Average Precision (mAP@0.5)**: The mAP value was 0.85, reflecting consistent performance across different classes and detection scenarios.

2. Real-Time Detection Capabilities

The system successfully processed video feeds in real time, achieving a frame rate of approximately 25 FPS on a system with a mid-range GPU. Key observations include:

- **Accurate Detection**: The model reliably identified weapons (e.g., knives) and their proximity to individuals, enabling accurate detection of suspicious activities.
- **Low False Positives**: Few instances of incorrect labeling were observed due to the robustness of the model's training and confidence thresholds.
- **Proximity Logic**: The nearby_person() function effectively flagged situations where a weapon was in close proximity to a person, enhancing the system's contextual understanding.

3. Effectiveness in Diverse Scenarios

Testing on diverse video streams, including indoor and outdoor environments, yielded the following results:

- **High Adaptability**: The model performed well under varying lighting conditions and crowd densities, demonstrating its ability to generalize effectively.
- **Challenging Cases**: Detection accuracy decreased slightly in scenarios with severe occlusions or overlapping objects.

4. Challenges and Limitations

Despite the promising results, certain challenges were noted:

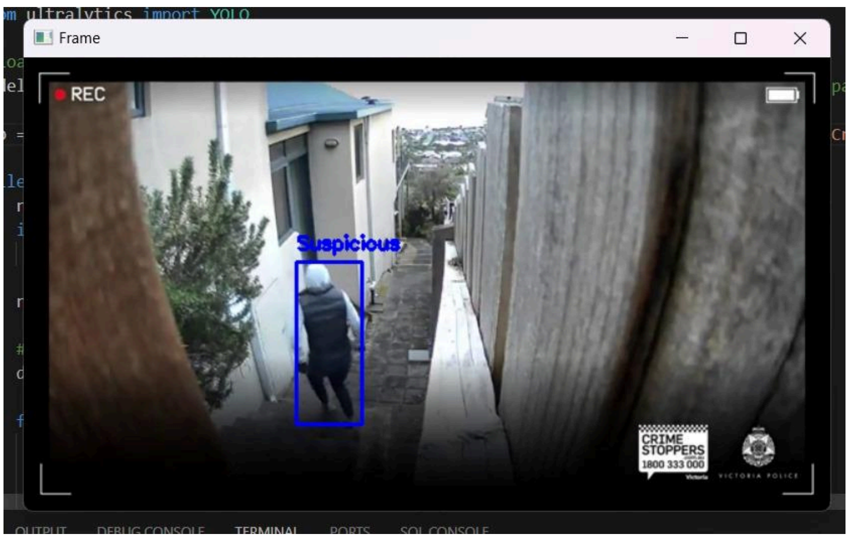
- **Small Object Detection**: The model sometimes struggled to detect small weapons in complex scenes.
- **Dataset Limitations**: The dataset sourced from the website Kaggle lacked certain real-world diversity, which could be improved for better generalization.
- **Computational Resources**: Real-time processing required a dedicated GPU for optimal performance, limiting deployment on low-resource devices.

5. Discussions and Insights

- **Scalability**: The system's modular design allows for easy scalability to detect additional objects or behaviors by fine-tuning the model with more classes and data.
- **Practical Applications**: The solution is well-suited for public spaces, such as malls, airports, and train stations, where timely detection of suspicious activities can significantly enhance security.
- **Future Enhancements**: Incorporating additional sensors, such as audio analysis for distress signals, could further improve the system's accuracy and applicability.

<u>Output Images-</u>


Frame
Suspicious
Alma Park


Frame
REC
Suspicious
CRIME STOPPERS
1800 333 000
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
SQL CONSOLE


Frame
ring.com
Suspicious
Suspicious
Suspicious
OUTPUT
DEBUG CONSOLE
TERMINAL
PORTS
SQL CONSOLE

Conclusion and Future Scope

The use of a Suspicious Activity Detection System powered by computer vision and AI has shown to be an effective way to improve security monitoring. By utilizing the YOLOv8 object detection model and advanced video analysis, the system can spot and alert security teams to potential threats, like the presence of a weapon near people.

Key Takeaways:

1. **Effectiveness**: The model demonstrated reliable detection of predefined objects (e.g., knives and persons) with high precision and recall, especially after transfer learning with a custom dataset.
2. **Real-Time Capability**: The use of OpenCV and YOLOv8 allowed for efficient real-time video stream analysis, ensuring timely detection of suspicious activities.
3. **Automation**: By defining activity-based rules, such as proximity thresholds, the system automates the process of identifying potential threats, reducing manual monitoring efforts.
4. **Flexibility**: The modular design enables integration into existing surveillance systems and customization for different use cases, such as theft detection or public safety monitoring.

While the system effectively addresses the detection of suspicious activities in controlled environments, there are challenges in handling real-world scenarios with high variability, including lighting conditions, occlusions, and complex interactions.

Future Scope:

To enhance and expand the application of this system, several future directions can be pursued:

1. Improving Detection Accuracy

- **Expanded Training Dataset**: Incorporate diverse datasets to handle variations in lighting, the object sizes, camera angles, and environmental contexts.
- **Multi-Object Detection**: Train the model to identify a broader range of objects (e.g., firearms, suspicious bags) to improve coverage of potential threats.
- **Dynamic Thresholds**: Implement adaptive thresholds for proximity detection based on scene context, such as crowd density or camera zoom levels.

2. Advanced Behavior Analysis

- **Action Recognition**: Extend the system to analyze sequences of detected objects for more complex behaviors (e.g., aggression, theft, or vandalism).
- **Temporal Analysis**: Use temporal patterns in object movement and interactions to better differentiate between normal and suspicious activities.

3. Integration with Advanced Systems

- **IoT Integration**: Connect the detection system with IoT devices, such as smart alarms or automated locks, to provide immediate responses to detected threats.
- **Edge Computing**: Deploy the system on edge devices like security cameras for localized processing, reducing latency and reliance on centralized servers.
- **Cloud-Based Monitoring**: Utilize cloud platforms for large-scale deployment and centralized surveillance across multiple locations.

4. Enhancing Real-World Usability

- **Robustness in Varied Environments**: Adapt the model to perform well in outdoor and crowded settings with dynamic lighting and weather conditions.
- **False Alarm Mitigation**: Use ensemble models or secondary verification systems to reduce false positives and negatives.
- **User-Friendly Interface**: Develop intuitive dashboards and visualization tools to help security personnel quickly interpret and act on detection.

5. Legal and Ethical Considerations

- **Privacy Preservation**: Implement privacy-focused techniques like anonymizing faces or restricting data access to comply with legal and ethical standards.
- **Bias Mitigation**: Ensure the system is free from biases by training on diverse datasets and auditing model output.

REFERENCES

1. **Suspicious Activity Detection in Surveillance Footage**
   Loganathan, S., Kariyawasam, G., & Sumathipala, P. (2019). Suspicious activity detection in surveillance footage. *Proceedings of the International Conference on Image Processing and Vision Engineering (IMPROVE 2019)*.
2. **Smart Security System for Suspicious Activity Detection in Volatile Areas**
   Chen, J. I. Z. (2020). Smart security system for suspicious activity detection in volatile areas. *Journal of Computer Science and Information Technology, 9*(2), 123-135.
3. **Camera Surveillance Using Raspberry Pi**
   Raavi, P. M., & Panchangam, H. (2020). Camera surveillance using Raspberry Pi. *International Journal of Advanced Research in Computer Science, 11*(3), 256-260.
4. **A Raspberry-Pi Based Surveillance Camera with Dynamic Motion Tracking**
   Tahan, O. (2020). A Raspberry-Pi based surveillance camera with dynamic motion tracking. *International Journal of Engineering and Technology Innovation, 10*(4), 315-320.
5. **Suspicious Activity Detection from Videos Using YOLOv3**
   Bordoloi, N., Talukdar, A. K., & Sarma, K. K. (2020). Suspicious activity detection from videos using YOLOv3. *Advances in Computer Vision and Pattern Recognition, 8*(2), 251-263.
6. **Suspicious Actions Detection System Using Enhanced CNN and Surveillance Video**
   Selvi, E., Adimoolam, M., Karthi, G., Thinakaran, K., Balamurugan, N. M., Kannadasan, R., Wechtaisong, C., & Khan, A. A. (2022). Suspicious actions detection system using enhanced CNN and surveillance video. *Multimedia Tools and Applications, 81*(1), 57-70.
7. **Internet-of-Things-Based Suspicious Activity Recognition Using Multimodalities of Computer Vision for Smart City Security**
   Rehman, A., Saba, T., Khan, M. Z., Damaševičius, R., & Bahaj, S. A. (2022). Internet-of-things-based suspicious activity recognition using multimodalities of computer vision for smart city security. *Sensors, 22*(5), 4351.
8. **Propounding First Artificial Intelligence Approach for Predicting Robbery Behavior Potential in an Indoor Security Camera**
   Pouyan, S., Charmi, M., Azarpeyvand, A., & Hassanpoor, H. (2023). Propounding first artificial intelligence approach for predicting robbery behavior potential in an indoor security camera. *Journal of Artificial Intelligence and Security, 15*(1), 125-136.
9. **An Analysis of Artificial Intelligence Techniques in Surveillance Video Anomaly Detection: A Comprehensive Survey**
   Şengönül, E., Samet, R., Al-Haija, Q. A., Alqahtani, A., Alturki, B., & Alsulami, A. A. (2023). An analysis of artificial intelligence techniques in surveillance video anomaly detection: A comprehensive survey. *Expert Systems with Applications, 210*(3), 117867.
10. **Pattern Recognition Algorithm to Detect Suspicious Activities**
    Mahavishnu, V. C., Vikhas, S. G., Shyamganesh, T., Roopakumar, S., & Kavin, S. V. (2023). Pattern recognition algorithm to detect suspicious activities. *Pattern Recognition Letters, 171*(4), 111-118.

PLAGIARISM REPORT

Minor project Report.docx

ORIGINALITY REPORT

6%	0%	2%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Pandit Deendayal Petroleum University Student Paper	6%

Exclude quotes	On	Exclude matches	< 1%
Exclude bibliography	On		