INCORPORATING DEEP LEARNING TO DETECT SUSPICIOUS ACTIVITY

S.Gayathri[1], K.N.S.S.Anvitha[2], P.Sai Meghana[3], N.Naveena Chowdary [4], M.Priyanka [5]
[1,2,3,4,5]Department of Computer Science and Engineering, Vignan's Institute of Engineering forWomen, Visakhapatnam, Andhra Pradesh, India

ABSTRACT

The project endeavors to fortify safety and security measures by implementing an intelligent surveillance system capable of detecting suspicious weapons and activities in real time using Closed-circuit Television (CCTV). The core technology employed is Deep Learning and Computer Vision, specifically leveraging the YOLOv8 model for robust object detection, targeting weapons such as guns and knives, as well as discerning suspicious human activities. Various Python libraries play pivotal roles in the project's implementation, including ultralytics for managing the YOLO model, cv2 (OpenCV) for image and video processing, and mathematical operations facilitated by the math library. Additionally, time it is utilized for measuring execution durations, while email. Mime and Twilio. Rest enables seamless communication by facilitating the sending of email and SMS alerts, respectively, leveraging Twilio's API for SMS messaging.

Keywords: Deep Learning, Computer Vision, YOLOV8,Suspicious Activity, Live Surveillance.

INTRODUCTION

In contemporary society, ensuring public safety and security stands as a paramount concern, prompting the widespread adoption of surveillance systems, particularly Closed-circuit Television (CCTV). While these systems serve as invaluable tools for monitoring public spaces, they often face a critical limitation: the inability to proactively detect and respond to suspicious activities in real-time. Moreover, the unpredictable nature of human behavior further compounds this challenge, as distinguishing between normal and suspicious activities becomes increasingly difficult. Recognizing these shortcomings, our project seeks to address this pressing issue by harnessing the power of advanced technologies, specifically Deep Learning and Computer Vision.

LITERATURE SURVEY

1.Title: "Deep Learning-Based Anomaly Detection for Video Surveillance: A Comprehensive Survey"

Authors: Nguyen, Minh; Tran, Linh

This survey paper comprehensively reviews deep learning-based approaches for anomaly detection in video surveillance. It examines various techniques, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs), highlighting their effectiveness in detecting suspicious activities such as abnormal behavior, intrusion, and vandalism.

It does not delve deeply into specific implementation challenges or comparative performance analysis of different deep learning models in surveillance applications.

2. Title: "Real-Time Suspicious Activity Detection in Crowded Scenes Using Convolutional Neural Networks"

Authors: Wang, Michael; Chen, Sarah

They proposed a real-time suspicious activity detection system using convolutional neural networks (CNNs) in crowded scenes. They focus on leveraging deep learning techniques to accurately identify anomalous behaviors, including aggressive movements, theft, and vandalism, in dense and dynamic environments captured by surveillance cameras.

The study lacks detailed analysis of the computational and resource requirements for real-time implementation of the proposed system, and it does not address challenges related to occlusions and variations in lighting conditions.

3. Title: "Efficient Deep Learning Models for Suspicious Activity Detection in Surveillance Videos"

Authors: Li, Kevin; Zhang, Sophia

It focuses on the development of efficient deep learning models for suspicious activity detection in surveillance videos. They emphasize lightweight architectures and model compression techniques to enable real-time processing of high-resolution video streams without compromising detection accuracy. They address challenges such as limited computational resources and bandwidth constraints in surveillance systems.

While the study focuses on efficiency, it does not provide a comparative analysis of the trade-offs between model complexity, detection accuracy, and computational efficiency. Moreover, it does not explore the robustness of the proposed models to adversarial attacks or environmental factors.

EXISTING METHOD

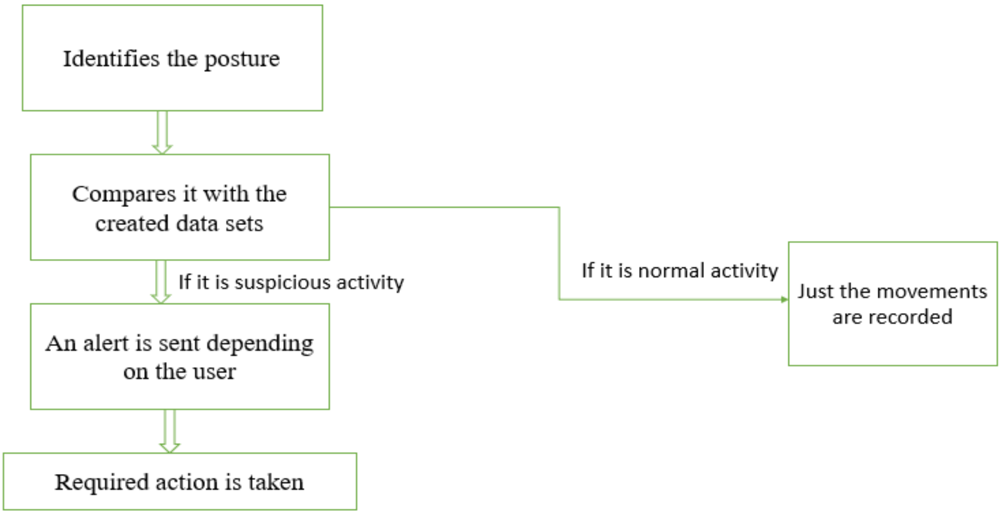
The existing surveillance system primarily relies on Closed-circuit Television (CCTV) cameras deployed in various public spaces, such as airports, train stations, malls, and streets, to monitor and record activities. These CCTV cameras continuously capture video footage, which is then stored for later review and analysis.

In the current system, the monitoring of CCTV footage is predominantly manual, with security personnel tasked with observing video feeds in real time or reviewing recorded footage after the fact. However, this manual monitoring process is labor intensive, time consuming, and prone to human error. Existing system lacks sophisticated algorithms or technologies to autonomously identify and flag potential security threats, such as the presence of weapons or suspicious behavior by individuals. While the existing surveillance system provides valuable monitoring capabilities, it falls short in terms of real-time threat detection and proactive security measures.

PROPOSED METHOD

In today’s world, we can see that crime has escalated despite the presence of surveillance cameras everywhere. To detect suspicious behavior, a model must be developed that reduces the time taken to detect it so that we can take action. So, we can use YOLO, Once the model is trained, we can deploy it in a real-time monitoring system. This system will continuously analyze incoming video streams, applying the YOLO v8 model to detect and predict any suspicious behavior. When a potential threat is identified, the system can generate email and alert notifications. YOLO is best for faster inference due to a single forward pass, its well suited for real time applications and its efficient at detecting multiple objects.

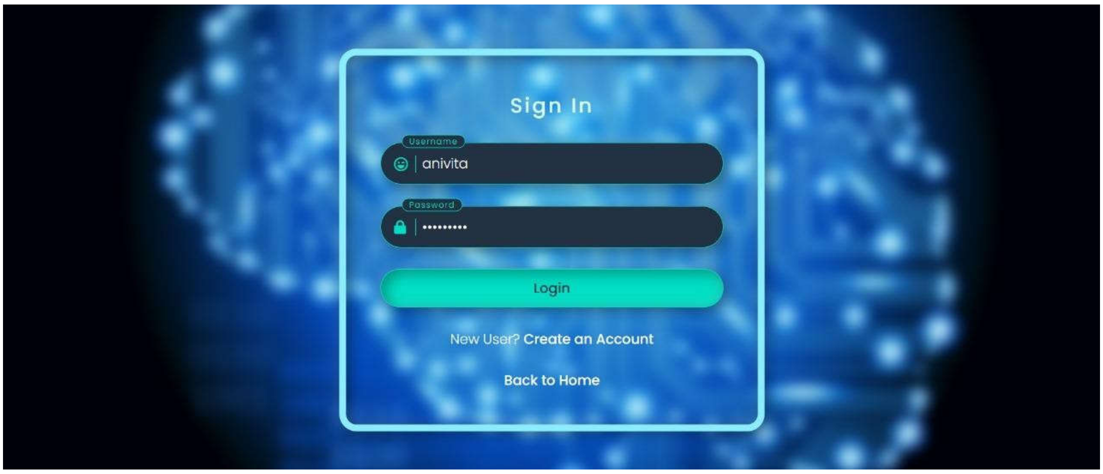
SYSTEM BLOCK DIAGRAM


Identifies the posture
Compares it with the created data sets
If it is suspicious activity
If it is normal activity
Just the movements are recorded
An alert is sent depending on the user
Required action is taken

1. Posture Identification:
The process begins by identifying the posture of an individual. This could involve analysing body position, movement, or specific gestures.
2. Comparison with Datasets:
The identified posture is compared with created datasets. These datasets likely contain examples of both normal and suspicious postures.
3. Suspicious Activity Check:
If the posture aligns with suspicious activity, an alert is sent to security personnel or relevant authorities. Required action is then taken based on the situation. If the posture is deemed normal activity, only the movements are recorded, without triggering an alert.
4. Overall Purpose:
The purpose of this process is likely to enhance security and surveillance systems by automating the detection of potentially harmful behaviour.

RESULT ANALYSIS:

1. Login Page



Sign In

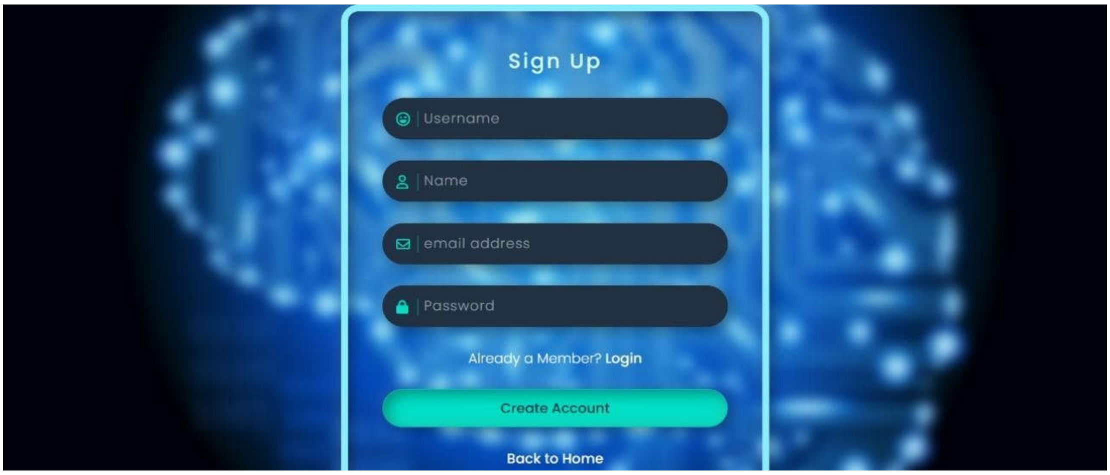
Username

anivita

Password

•••••••••

2. Register Page



Sign Up

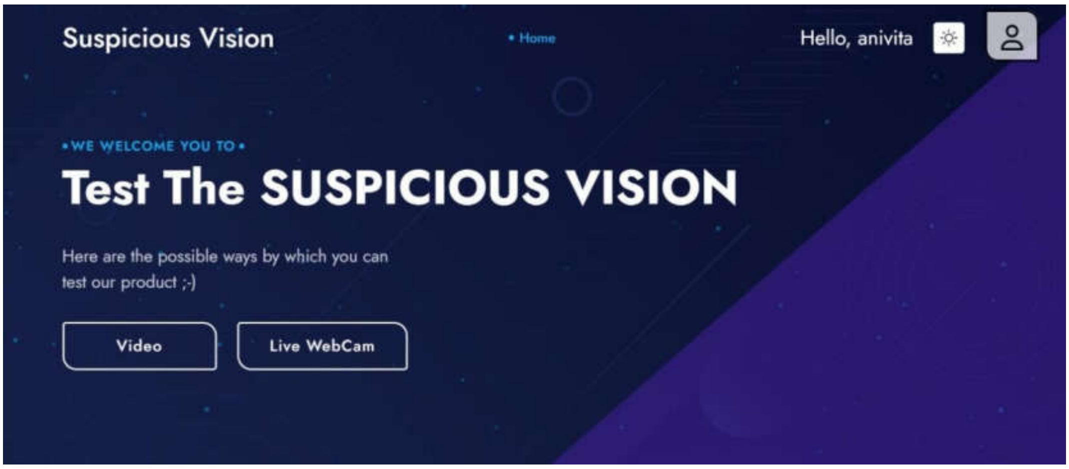
Username

Name

email address

Password

3. Home Page

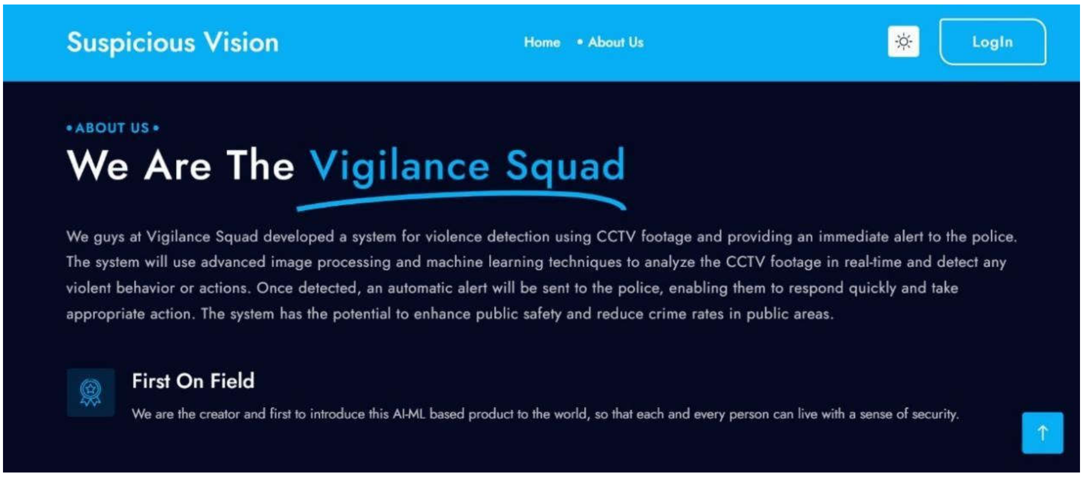


• WE WELCOME YOU TO •

Test The SUSPICIOUS VISION

Here are the possible ways by which you can test our product ;-)

4. About Us Page



•ABOUT US•

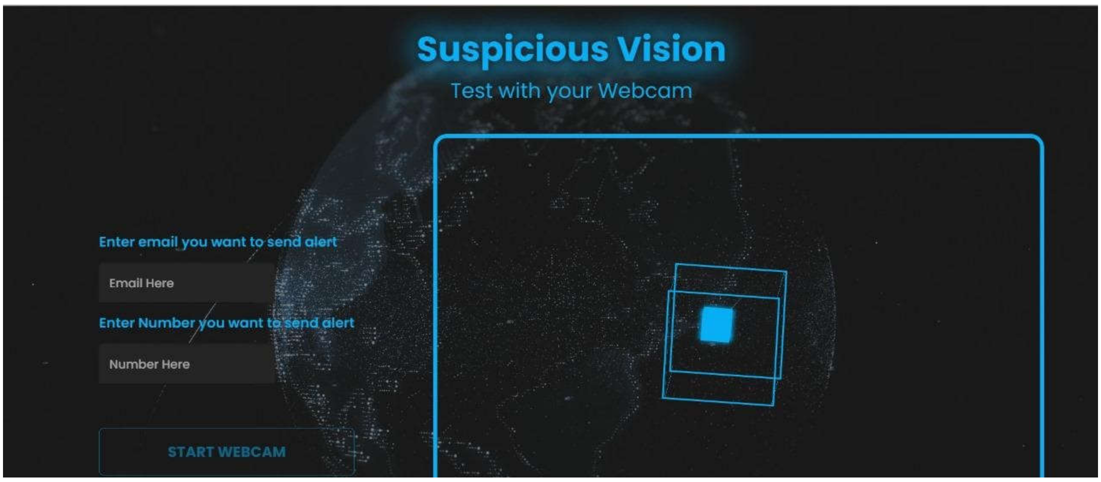
We Are The Vigilance Squad

We guys at Vigilance Squad developed a system for violence detection using CCTV footage and providing an immediate alert to the police. The system will use advanced image processing and machine learning techniques to analyze the CCTV footage in real-time and detect any violent behavior or actions. Once detected, an automatic alert will be sent to the police, enabling them to respond quickly and take appropriate action. The system has the potential to enhance public safety and reduce crime rates in public areas.

First On Field

We are the creator and first to introduce this AI-ML based product to the world, so that each and every person can live with a sense of security.

5. Test WebCam Page

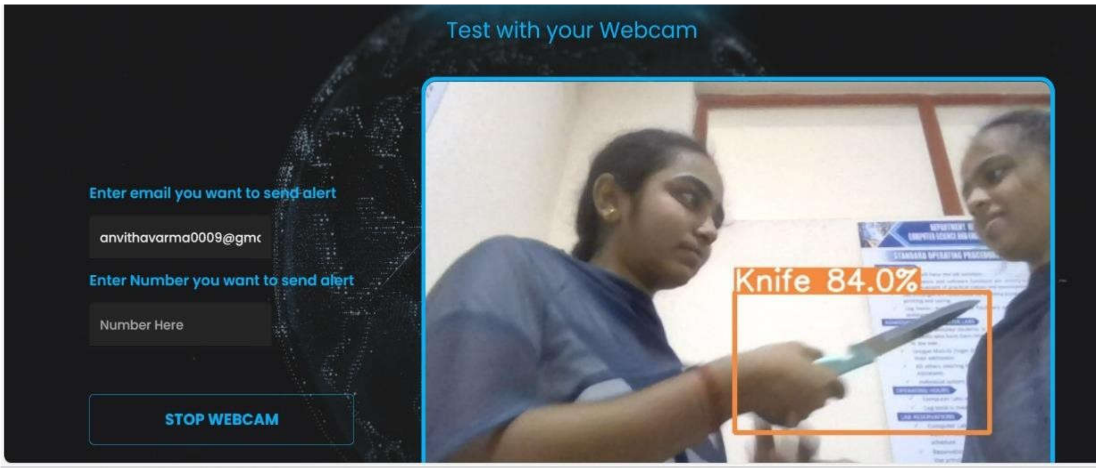


Enter email you want to send alert

Email Here

Enter Number you want to send alert

Number Here



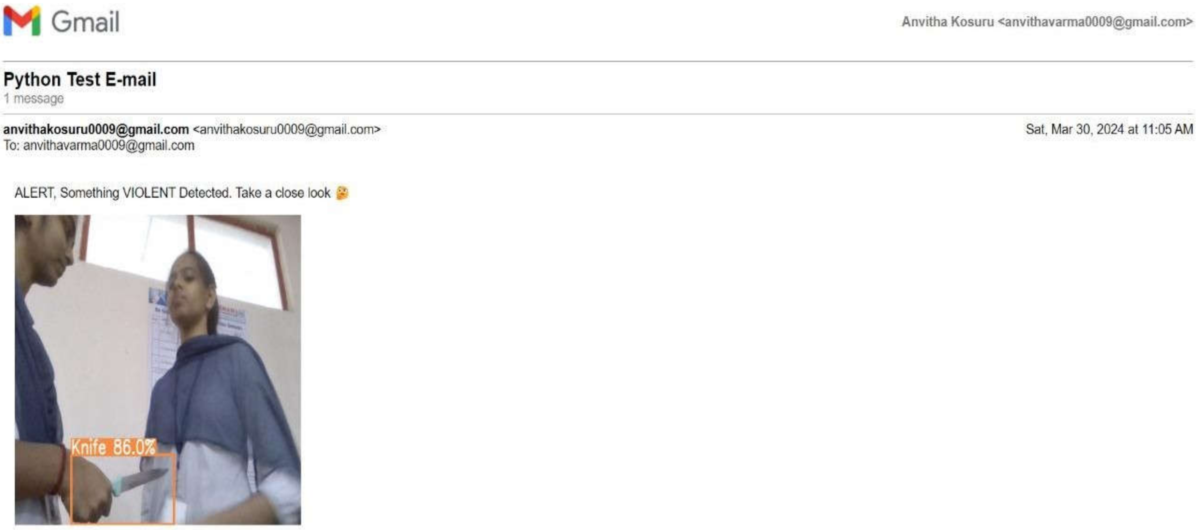
Enter email you want to send alert

anvithavarma0009@gmc

Enter Number you want to send alert

Number Here

6. Mail Sent to authorities



Anvitha Kosuru <anvithavarma0009@gmail.com>

Python Test E-mail
1 message

anvithakosuru0009@gmail.com <anvithakosuru0009@gmail.com> Sat, Mar 30, 2024 at 11:05 AM
To: anvithavarma0009@gmail.com

ALERT, Something VIOLENT Detected. Take a close look 🤔

CONCLUSION

Implementation of the intelligent surveillance system demonstrates the efficacy of leveraging deep learning and computer vision technologies to enhance security measures. By utilizing YOLOv8 for real-time object detection and behavior analysis, the system can accurately detect and alert authorities to suspicious activities and objects in surveillance footage. The integration of email, SMS, and possibly WhatsApp notifications ensures timely dissemination of alerts, enabling swift response to potential security threats. Additionally, the development of a user-friendly web interface provides security personnel with easy access to monitoring and management tools, facilitating efficient oversight of surveillance operations. Overall, the intelligent surveillance system represents a significant advancement in security technology, offering robust detection capabilities, rapid alerting mechanisms, and streamlined monitoring processes. As security concerns continue to evolve, the system stands ready to adapt and evolve alongside emerging threats, safeguarding lives and property with cutting-edge surveillance solutions.

REFERENCES

[1] Monika D. Rokade and Tejashri S. Bora, "Survey on Anomaly Detection for Video Surveillance" 2021 International Research Journal of Engineering and Technology (IRJET).

[2] Jefferson Ryan Medel, Andreas Savakis, “Anomaly Detection in Video Using Predictive Convolutional Long Short-Term Memory Networks” under review.

[3] J. R. Medel and A. Savakis, “Anomaly detection in video using predictive convolutional long short-term memory networks,” arrive preprintarXiv:1612.00390, 2016.

[4] Bhagya Divya, Shalini, R.Deepa, Baddeli Sravya Reddy,“Inspection of suspicious human activity in the crowdsourced areas captured in surveillance cameras”,International Research Journal of Engineering andTechnology (IRJET),December 2017.

[5] Jitendra Musale,Akshata Gavhane, Liyakat Shaikh, Pournima Hagwane, Snehalata Tadge, “Suspicious Movement Detection and Tracking of Human Behavior and Object with Fire Detection using A Closed Circuit TV (CCTV) cameras ”, International Journal for Research in Applied Science & Engineering Technology (IJRASET) Volume 5 Issue XII December 2017.

[6] Elizabeth Scaria, Aby Abahai T and Elizabeth Isaac, “Suspicious Activity Detection in Surveillance Video using Discriminative Deep Belief Netwok”, International Journal of Control Theory and Applications Volume 10.

[7] Amrutha C.V, C. Jyotsna, Amudha J. “Machine Learning Approach for Suspicious Activity Detection from Surveillance Video” , IEEE Xplore , Issue 23 April 2020

[8] Phalguni Kadam , Shweta Gawande , Akshita Thorat , Rohini Mule. “Suspicious Activity Detection using Image Processing”, Journal of Science and Technology, Issue 01, August 2021.