ANOMALY DETECTION SYSTEM

Prof. Uttam Patole[1], Nilesh Gorhe[2], Kunal Chavan[3], Pranav Kulkarni[4], Janvi Dale[5]

*[1]Assistant Professor, Department of Computer Engineering, Sir Visvesvaraya Institute Of Technology, Nashik, Maharashtra, India.
*[2,3,4,5]Student, Department of Computer Engineering, Sir Visvesvaraya Institute Of Technology, Nashik, Maharashtra, India.

---***---

Abstract - In an era marked by dynamic security challenges, real-time CCTV anomaly detection systems have emerged as a cornerstone in contemporary security frameworks. These systems, leveraging advanced algorithms rooted in machine learning, continuously scrutinize live video streams to establish a baseline of normal activities. The fundamental aim is to promptly identify deviations and anomalies, ushering in a new era of proactive and responsive security monitoring. This technology's real-time capabilities represent a transformative leap forward, enabling immediate responses to potential threats or irregular events within monitored environments. The effectiveness of real-time anomaly detection lies not only in its ability to distinguish between normal and abnormal patterns but also in its contribution to the broader landscape of safety and protection. This abstract delves into the multifaceted significance of real-time CCTV anomaly detection, exploring its role in elevating overall security measures. Beyond the immediate identification of anomalies, these systems promise to shape the future of security by offering a proactive approach to surveillance. As technological advancements persist, the integration of such systems underscores a commitment to anticipatory security strategies, ensuring adaptability in the face of evolving security challenges.

Keywords: Anomaly Detection, Intrusion Detection, Machine Learning, Statistical Methods, Network Security, Cybersecurity, Pattern Recognition, Alarm Systems, Real-time Detection.

1. INTRODUCTION

In the contemporary landscape of security and surveillance, the integration of real-time CCTV anomaly detection systems represents a paradigm shift in how we approach the challenges of monitoring dynamic environments. These systems, underpinned by sophisticated algorithms with a foundation in machine learning, have redefined our ability to analyze live video streams continually. By establishing a baseline of normal activities, these systems empower security professionals with the capability to promptly identify deviations and anomalies, introducing a new era of proactive and responsive security monitoring. The core objective of real-time CCTV anomaly detection is to transcend traditional surveillance methods, offering an intelligent and adaptive approach to security. As the prevalence of security threats becomes increasingly diverse and complex, the need for advanced monitoring technologies becomes imperative. Real-time anomaly detection systems not only keep pace with these challenges but also provide a predictive layer, allowing for pre-emptive responses to potential security breaches or unusual events within the monitored environment. The effectiveness of real-time anomaly detection lies not only in its ability to distinguish between normal and abnormal patterns but also in its contribution to the broader landscape of safety and protection. This abstract delves into the multifaceted significance of real-time CCTV anomaly detection, exploring its role in elevating overall security measures.

A. Problem Statement

Designing an effective anomaly detection system involves developing algorithms and techniques capable of accurately identifying anomalies within large datasets in real-time or near real-time. The system should be able to adapt to dynamic environments where normal behavior may evolve over time and where anomalies may take various forms.

B. Project Scope

In the Anomaly Recognition System, the challenging part is the real-time execution of the model. A more effective and cost-efficient solution can be implemented in the future to overcome this. The model can also be augmented to discover a potential threat and alert the authorities in advance of the incoming threat hence, increasing the safety of people.

Main point:

- It resolves the security concerns.
- It uses advanced machine learning algorithms to recognize the anomalies.
- Higher response than other surveillance systems.

Assumptions and Dependencies:

- **Camera Functionality:** Assumption that CCTV cameras are fully functional, regularly maintained, and provide clear and reliable video feeds.
- **Network Infrastructure:** Assumption that a stable and secure network infrastructure is in place to support the real-time streaming and communication requirements of the system.
- **Data Quality:** Assumption that incoming video data is of sufficient quality and clarity for effective anomaly detection, with minimal artifacts or distortions.
- **Access to Historical Data:** Assumption that historical data for baseline learning is available and representative of normal behaviors within the monitored environment.

2. SYSTEM ARCHITECTURE

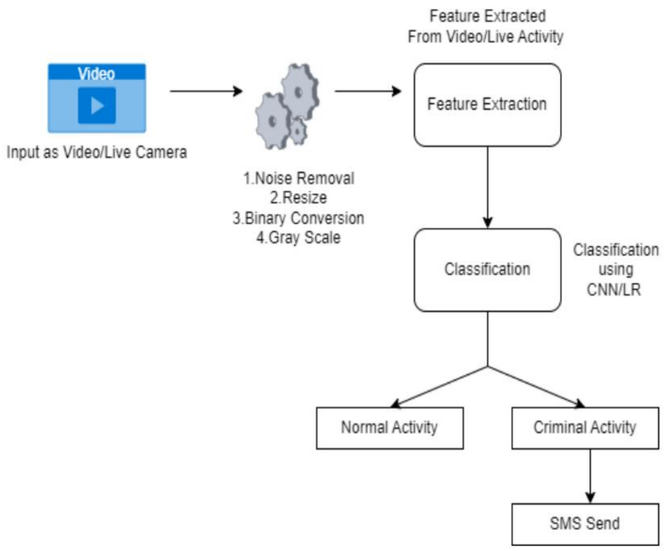


Fig -1: Architecture Diagram

The real-time CCTV anomaly detection system is structured with a comprehensive architecture to efficiently monitor and analyze live video streams for potential anomalies. The key components of this system architecture include:

Video Input Module: This module serves as the starting point, capturing live video feeds from CCTV cameras deployed in the monitored area. The video input provides the raw data for subsequent processing.

Feature Extraction Module: The Feature Extraction Module identifies essential information from video frames, such as shapes, colors, and motion patterns. These features are crucial for building a comprehensive understanding of the monitored environment.

Anomaly Detection Algorithm Module: The Anomaly Detection Algorithm Module employs statistical methods or machine learning models to analyze the features extracted. It compares observed patterns with the learned baseline to detect significant deviations, indicating potential anomalies.

Real-time Analysis Module: Operating in real-time, this module continuously evaluates video streams for anomalies. It promptly triggers alerts or notifications when deviations from the established baseline are identified, ensuring immediate responsiveness.

User Interface Module: The User Interface Module provides a graphical interface for system administrators and security personnel to monitor the system. It typically includes a dashboard displaying live video feeds, alert logs, and system configuration options.

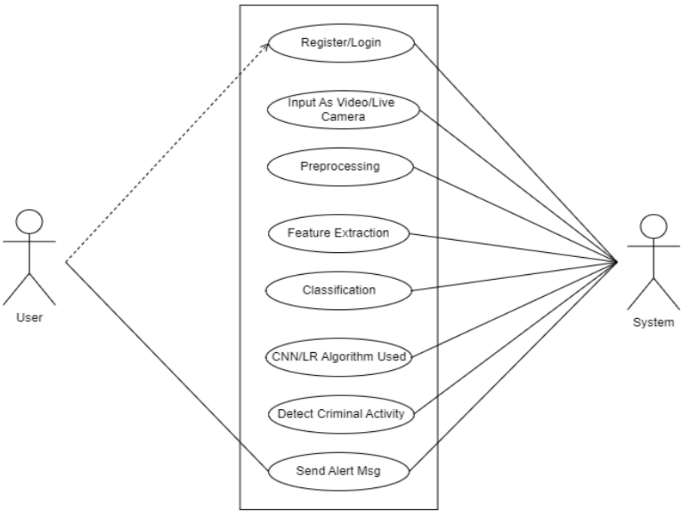


Fig -2: Use-Case Diagram

- Actors in the use case diagram are the System and User.
- User: Interacts with the anomaly detection system, may configure settings, register/login, send alert message/alarm, view results, or provide feedback.
- System Admin: Responsible for managing the system, setting up configurations, managing user access, etc.

3. FUNCTIONAL REQUIREMENTS

User-Interface-

Register:
In this interface, users will have to create an account. It will contain text fields user name, email address, enter password, and re-enter password. And one button "Create Account" to create an account.

Login:
This will consist of the login interface. It will contain text fields allowing user name and password for login with a corresponding button, a button for a help menu that will assist in usability, and a button that will allow the manager to reset the password. Depending on the type of user who logs on, either the admin or the user interface will be loaded.

Software Interface:

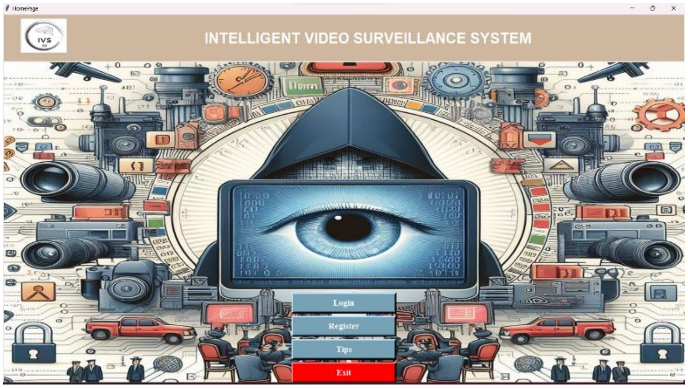
Application Based on Suspicious Activity Detection.

IDE: Spyder

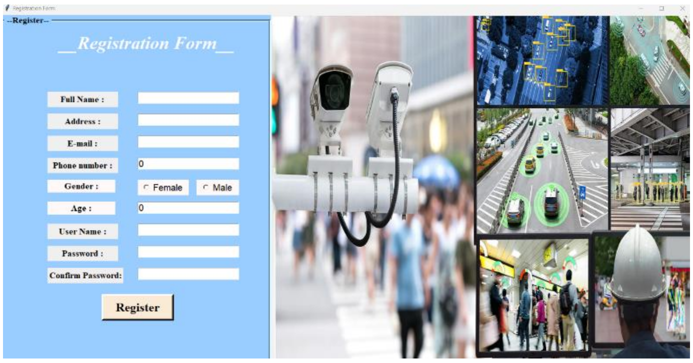
Programming language: Python

4. SNAPSHOOTS

-Home Page:

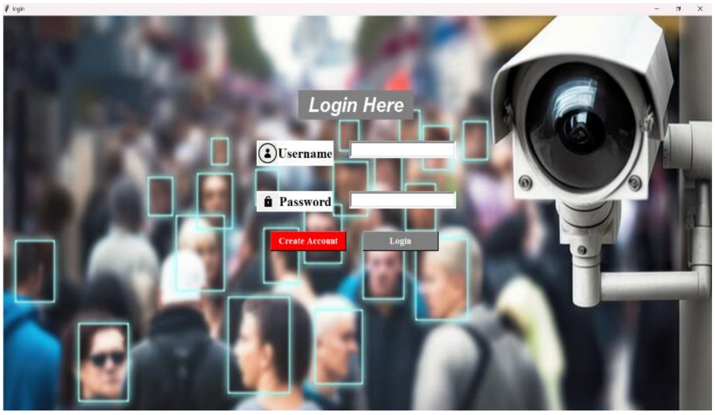


-Registration Page:

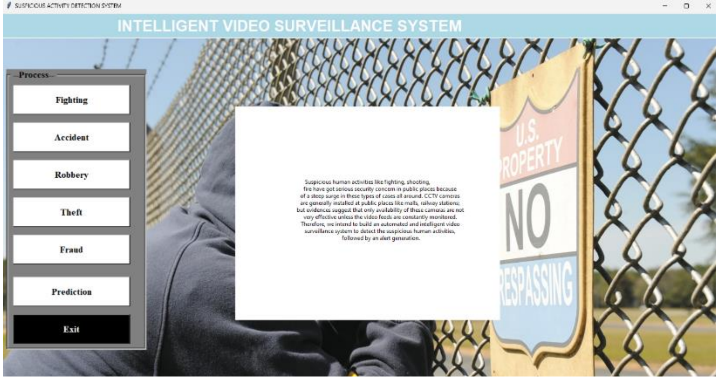


Full Name :
Address :
E-mail :
Phone number : 0
Gender : ○ Female ○ Male
Age : 0
User Name :
Password :
Confirm Password:

-Login Page:

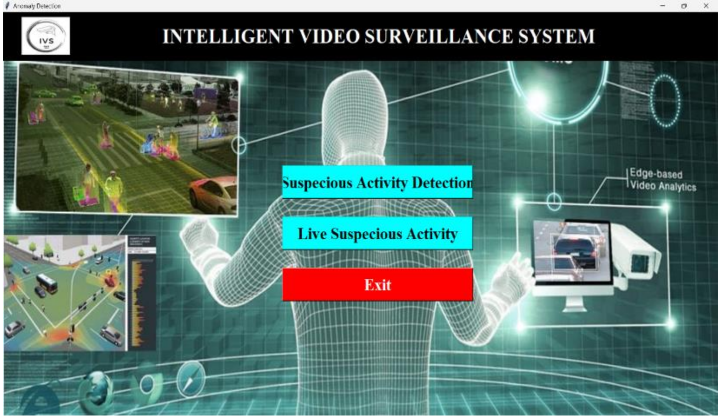


-Precautions Page:

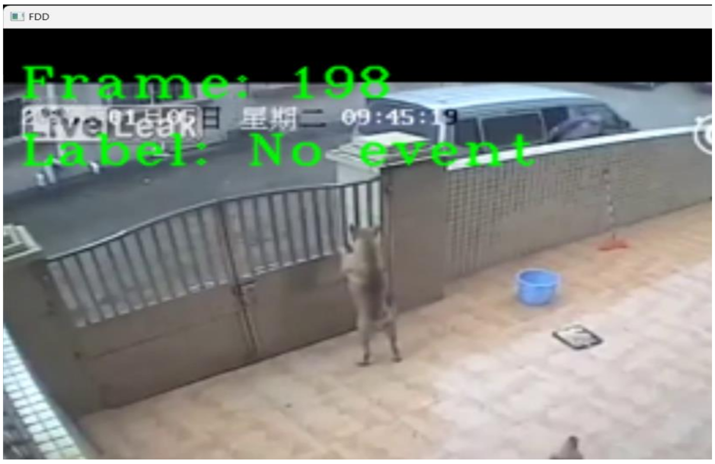


Suspicious human activities like fighting, shooting, fire have got serious security concem in public places because of a steep surge in these types of cases all around. CCTV cameras are generally installed at public places like malls, railway stations; but evidences suggest that only availability of these cameras are not very effective unless the video feeds are constantly monitored. Therefore, we intend to build an automated and intelligent video surveillance system to detect the suspicious human activities, followed by an alert generation.

-Main Page:

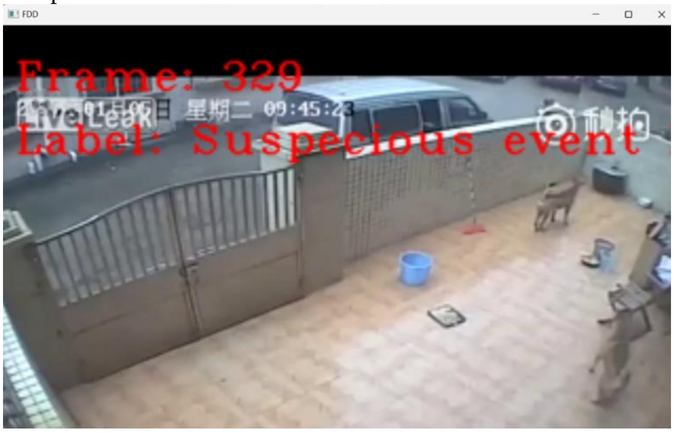

Anomaly Detection
IVS
INTELLIGENT VIDEO SURVEILLANCE SYSTEM
Suspicious Activity Detection
Live Suspecious Activity
Exit
Edge-based Video Analytics

-Normal Event:

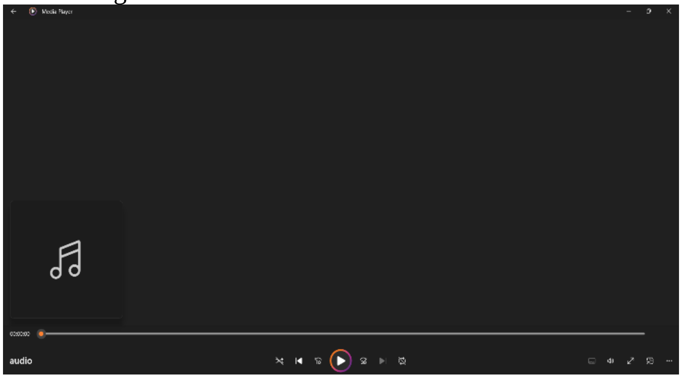


Frame: 198
Label: No event

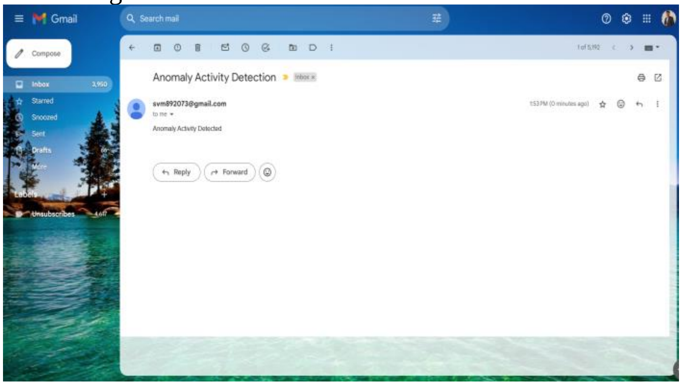
-Suspicious Event:



-Alarm Page:



-Email Page:



Anomaly Activity Detection

svm892073@gmail.com
to me

Anomaly Activity Detected

5. CONCLUSION

A system to process real-time CCTV footage to detect any suspicious activity will help to create better security and less human intervention. Great strides have been made in the field of human Suspicious Activity, which enables us to better serve the myriad applications that are possible with it. Moreover, research in related fields such as Activity Tracking can greatly enhance its productive utilization in several fields.

6. REFERENCES

1. A Powerful Technique for Maintaining Privacy of Images on Content Sharing Sites, UR Patole, NL Jain, TS Baviskar, GA Bhosale, SM Chaudhari [1]
2. BOT Virtual Guide, N Tungar, N Avhad, P Gayakhe, R Musmade, UR Patole. [2]
3. An Efficient Technique to Control Images on Content Sharing Sites, TS Bavisar, NL Jain, GA Bhosale, SM Chaudhari, UR Patole.[3]
4. Review 2 Smart Saline, UR Patole, SS Yeole, RS Patil, NR Kushwaha, VA Kankrej system4 (09) [4]
5. Sensor Based model for soil testing using machine learning, UR Patole, IJIRCCE 11 (2), 485-487. [5]
6. Lung X-Ray Image Enhancement to identify Pneumonia with CNN, UR Patole, SN Sakshi Kishor Jadhav, SN Mohommad Afraaz Firoz Khan, IJSRD 9 (ISSUE: 12), 45-51. [6]
7. Ecg Monitoring Using Smart Phone and Bluetooth, MN Gulve, MR Abhale, UR Patole, MD Kadri, MP Gugale Vidyawarta.[7]

7. AUTHORS BIOGRAPHY

	Prof. Uttam Patole (Assistant Professor of Computer Engineering Department)
	Mr. Nilesh Gorhe (BE Computer Engineering Student)
	Mr. Pranav Kulkarni (BE Computer Engineering Student)
	Mr. Kunal Chavan (BE Computer Engineering Student)
	Miss. Janvi Dale (BE Computer Engineering Student)