

INTRUDER DETECTION USING VIDEO SURVEILLANCE WITH CLOUD

Sd.Sameer Sulthan, Department of CSE, Narayana Engineering College, Gudur, India

Mrs.P.Madhavi, Assistant professor, Department of CSE, Narayana Engineering

College, Gudur, India

ABSTRACT

The project presents a comprehensive security system integrating object detection, face recognition, and email notification capabilities for real-time surveillance. Leveraging the YOLOv5 model for object detection, the system monitors a live video feed from a webcam to identify and track persons. The face recognition library is employed to perform facial recognition on detected individuals, comparing their features against a set of known faces.

Upon detecting an unrecognized person, the system captures an image of the intruder and initiates an email alert mechanism. The alert includes a time stamped image attachment and is sent to a specified email address, facilitating remote notification of security events. An additional layer of verification is introduced through the monitoring of incoming emails, allowing the system to confirm the validity of a person based on predefined subject criteria.

The project incorporates audible alarms using Pygame, providing an auditory cue for the presence of an intruder or the occurrence of specific events, such as the sending of email alerts. Continuous monitoring ensures a real-time response to security threats, with time stamped images logged for future analysis.

The system is designed for ease of use and adaptability, making it suitable for smallscale security surveillance applications. As an integrated solution, it combines cuttingedge object detection and facerecognition technologies with effective alerting mechanisms, enhancing the overall security posture. The project contributes to the field of surveillance systems by providing a practical and accessible solution for individuals seeking to implement advanced security measures in their environments.

INTRODUCTION:

In today's world, keeping people and places safe is crucial. This project aims to create a smart security system using advanced technologies to detect objects and recognize faces. This project uses a powerful tool called YOLOv5 to watch a live video from a webcam and quickly identify and track people. Another tool, face recognition, helps system to recognize familiar faces from strangers. One standout feature of this system is its ability to send alerts. If someone unfamiliar is detected, this system takes a picture and sends an email alert to a higher officials. This allows for quick responses to potential security issues.

To make the system even more reliable, system also checks incoming emails for specific information, adding an extra layer of confirmation about a person's identity. This project also includes audible alarms to the mix. These are sounds that can be heard, alerting people to the presence of someone unfamiliar or security setups. This system continuously monitor, send alerts in real-time, and keep a record of images with timestamps, providing a comprehensive security solution for everyday use.

As going through this report, we'll dive into more details about how the system works, what it can do, how it's built, and how well it performs. This will help us understand why this integrated security system is important and how it could be useful in different situations.

OBJECTIVE OF THE PROJECT:

- 1.Real-time Object Detection:** Develop a system capable of real-time object detection using YOLOv5 to identify and track persons within a live video feed from a webcam.
- 2.Facial Recognition:** Implement face recognition functionality utilizing the face recognition library to distinguish known faces from unrecognized individuals detected in the monitored space.
- 3.Proactive Alerting Mechanism:** Enable the system to initiate timely and proactive alerts by capturing images of unrecognized persons and sending email notifications to a predefined recipient.
- 4.Verification through Email:** Implement a verification mechanism by monitoring incoming emails for specific subject criteria, providing an additional layer of confirmation regarding the validity of detected individuals.
- 5.Audible Alarm Integration:** Incorporate audible alarms using Pygame to provide both visual and audible alerts, enhancing situational awareness and drawing attention to security events.
- 6.Continuous Monitoring:** Establish continuous monitoring of video feed, ensuring the system's ability to respond in real-time to potential security threats.
- 7.User-friendly Design:** The project's objectives aim to address the identified challenges in traditional security systems and deliver a practical, responsive, and user-friendly solution for enhancing security measures in both residential and commercial setting.

EXISTING SYSTEM IN PROJECT:

In recent years, the rapid evolution of technology has brought about sophisticated intruder detection systems using video surveillance, playing a vital role in enhancing security across residential, commercial, and public spaces. This analysis delves into various existing intruder detection systems, shedding light on their features, advantages, and limitations.

- 1.Traditional Motion Detection Systems:** Traditional systems, reliant on pixel value changes in video frames, are cost-effective but prone to high false alarm rates due to factors like lighting changes. Differentiating between intruders and other moving objects remains a challenge.
- 2.Infrared-Based Intruder Detection:** Infrared systems, using heat signatures to detect living beings, prove effective in low-light conditions but may trigger false alarms from non-human heat sources. Their application is limited due to range constraints.
- 3.Acoustic Intruder Detection Systems:** Acoustic systems, employing microphones to capture sounds associated with intruders, offer additional information but are susceptible to ambient noise. Lack of visual confirmation makes accurate identification challenging.
- 4.Video Analytics-Based Intruder Detection:** Video analytics systems, powered by machine learning algorithms, analyze behavior, size, and movement patterns. While advanced, they require significant computational power and accuracy hinges on training data quality.
- 5.Machine Learning and Deep Learning-Based Intruder Detection:** ML and DL techniques, especially using CNNs, significantly enhance accuracy by extracting complex features from video frames. Their adaptability to different environments and continuous improvement make them promising for modern surveillance.
- 6.Behavior Analysis and Pattern Recognition:** Advancements in behavior analysis and pattern recognition involve studying movement patterns for identifying deviations as potential intruders. This nuanced approach reduces false alarms and boosts system reliability.
- 7.Integration with IoT Devices:** Integrating intruder detection with IoT devices expands surveillance capabilities. Smart sensors and cameras collaborate to provide real-time data, enabling automated responses like lighting activation or security alerts.

Intruder detection systems have evolved from basic motion detection to sophisticated video analytics, offering higher accuracy. However, these advancements may come with increased costs and computational demands. It's crucial to note that no system is flawless, and factors such as cost, scalability, and specific security needs must be considered when choosing a system. Ongoing research and development are expected to yield more advanced intruder detection solutions, enhancing safety across diverse settings. Choosing the right system involves considering factors like application, budget, and desired accuracy, ensuring a balance between cost-effectiveness and practicality. Organizations and individuals should carefully evaluate these systems to meet their security needs while acknowledging the inherent limitations and benefits of each technology.

DESIGN AND IMPLEMENTATION:

UML DIAGRAMS

USECASE DIAGRAM:

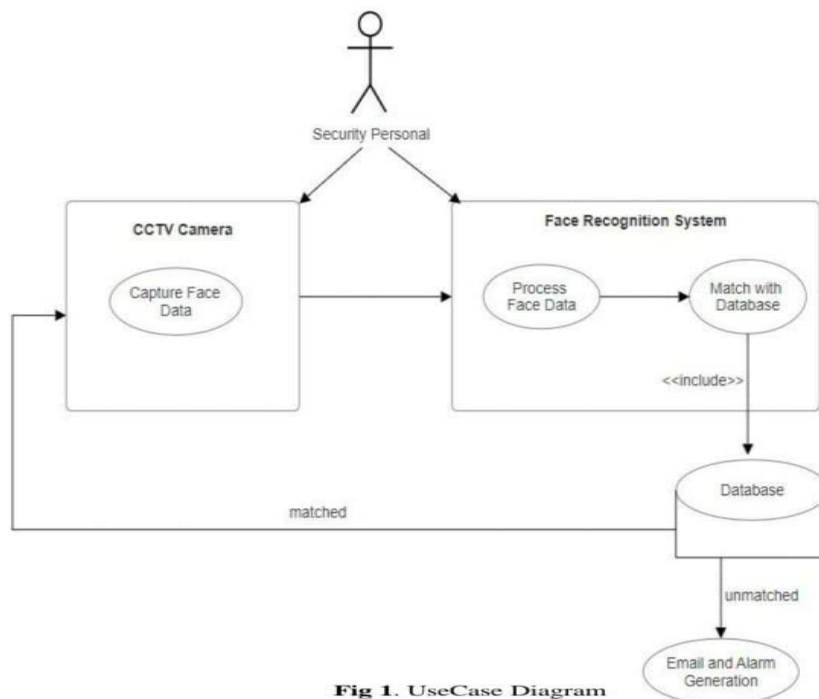


Fig 1. UseCase Diagram

1. Capture Face Data: This use case involves capturing facial data when a person enters the surveillance area. The camera is the primary actor responsible for capturing images or frames of the person's face. The person is a passive actor, being captured by the camera.

2. Process Face Data: This use case involves the processing system's role in analyzing the captured face data for person detection. YOLOv5 (or a similar detection model) is responsible for processing the face data and identifying whether it is a person or not.

3. Match with Database: In this use case, the processing system checks whether the detected person matches any records in the database of authorized individuals. It's a critical step for deciding whether the person is valid or not.

4. Database: The database use case represents the interaction with the database where authorized individuals' data, including their facial features, is stored. The database administrator is responsible for managing the database.

SEQUENCE DIAGRAM:

A Sequence Diagram is a visual representation that illustrates the interactions and communication between different components or objects in a system over a period of time. In the context of a surveillance and facial recognition system, let's create a sequence diagram for the process that involves the camera, preprocessing, feature extraction, checking the face in the database, and email and alarm generation. This sequence diagram illustrates the flow of events in the facial recognition process, from capturing a face with the Camera to the generation of email notifications and alarm triggers, depending on whether a match with the database is found.

The Sequence Diagram for the facial recognition process depicts the step-by-step interaction among system components. It begins with the Camera capturing a person's face, followed by preprocessing to optimize the image data. Feature extraction then extracts relevant facial features, which are compared to records in the Database. If a match is found, the Database signals the Email Module to generate

an email notification with the recognized person's identity. If no match occurs, the Database also triggers the Email Module but indicating an unauthorized access attempt. Simultaneously, the Alarm Module activates security measures, like sirens or lights, to deter unauthorized access. This sequence ensures real-time security and access control in the surveillance and facial recognition system.

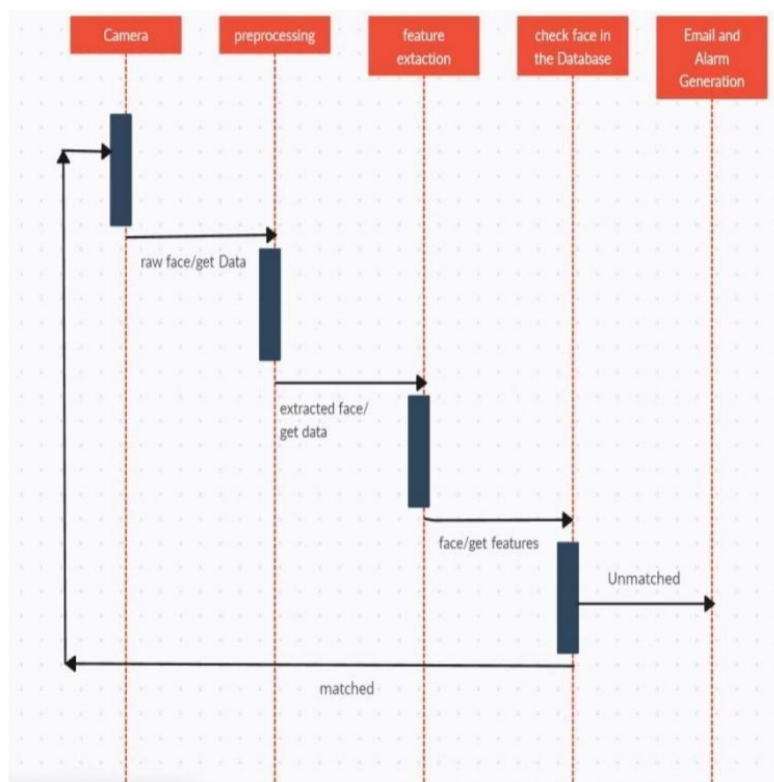


Fig 2: Sequence Diagram

ACTIVITY DIAGRAM:

An Activity Diagram is a visual representation of a workflow that illustrates the sequence of activities and decisions within a system or process. In the context of capturing and processing face data with conditional branches,

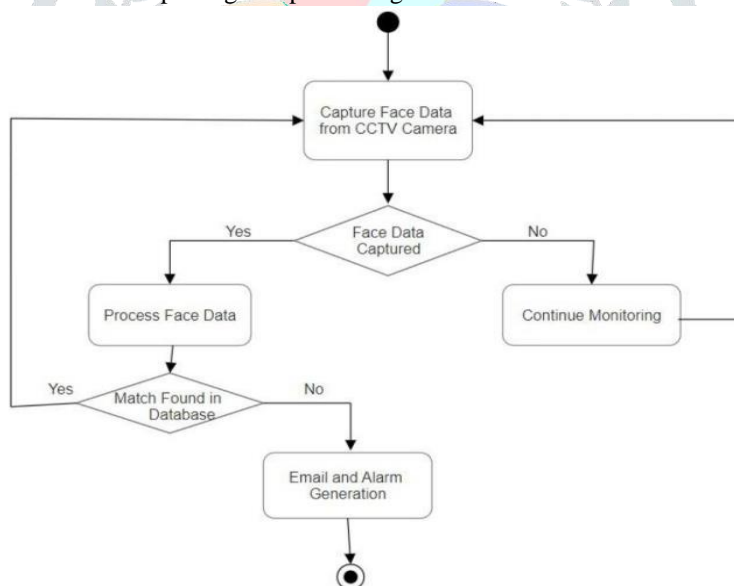


Fig3: Activity Diagram

TESTING:

Detected Images



Fig4: Identifying Person

The detected image is checked with our database, if the image matched with any image in the database then it continues the process again otherwise this images that are stored is sent to designated recipients. Hence these images are required to sent to the designated recipients.

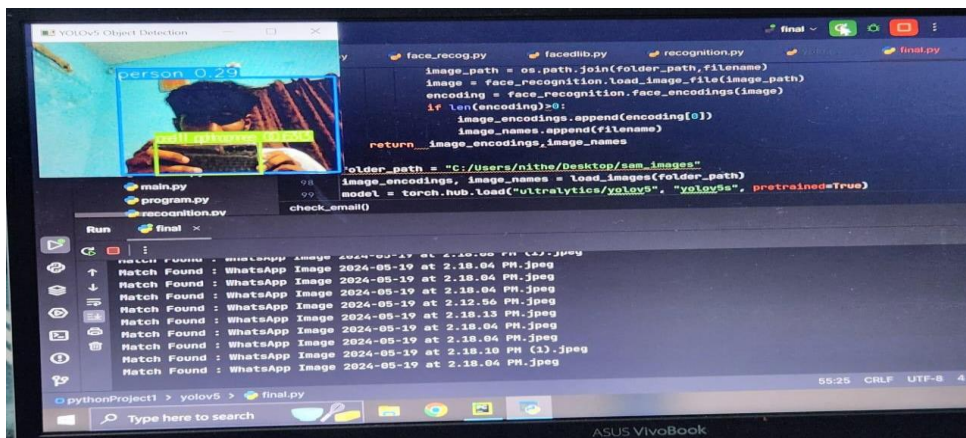


Fig5: Identifying the face in the detected person

From the above image we observe that Match Found : Image.jpg it means as the person is already in the database when the camera captures that person then it will generate as Match Found otherwise it will sent mail.

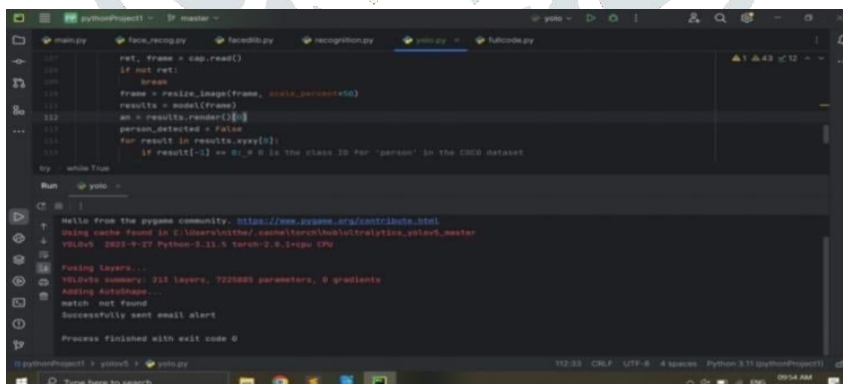


Fig6: Match not found Scenario(person not in database)

CONCLUSION:

Intruder detection through video surveillance, powered by the YOLOv5 model and complemented by alarm generation and email notifications, signifies a revolutionary advancement in modern security technology. This comprehensive approach not only swiftly identifies intruders in real-time but also facilitates immediate responses, establishing it as a cornerstone for robust security systems across diverse environments.

The utilization of the YOLOv5 model brings unparalleled accuracy and efficiency to intruder detection. Its rapid processing of video frames minimizes false alarms, allowing security personnel to concentrate on genuine threats. This integration highlights the pivotal role of cutting-edge machine learning in enhancing security, enabling proactive responses to potential breaches.

The activation of alarms upon detecting an intruder adds a layer of effectiveness to the system. Immediate alarm response not only alerts individuals nearby but acts as a powerful deterrent, discouraging intruders and preventing potential losses. This capability instills confidence in users, whether homeowners, business owners, or public space administrators, providing essential peace of mind in today's security-conscious world.

Real-time functionality enhances the system's effectiveness, with swift detection, assessment, and response capabilities. The instantaneous dissemination of information through email notifications ensures timely alerts to relevant individuals, enabling immediate action. This rapid communication is vital in preventing crimes, minimizing damages, and apprehending intruders promptly.

In conclusion, the integration of video surveillance, the YOLOv5 model, alarm generation, and email notifications marks a paradigm shift in security technology. This holistic approach, with its unmatched accuracy, proactive response, and seamless communication, emerges as an indispensable tool for ensuring safety and security across various environments. As technology evolves, the continued integration of advanced machine learning models and real-time communication methods is set to shape the future of intruder detection systems, enhancing security while providing peace of mind for individuals, businesses, and communities.

REFERENCES:

1. Wagh, K. S., et al. "Video Surveillance System in Bank for Analysis of Sentiment, Objects and Crowd Detection Using Deep Learning." 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), IEEE, 2023, pp. 911–19. DOI.org
2. Lohani, Devashish, et al. "Perimeter Intrusion Detection by Video Surveillance: A Survey." *Sensors*, vol. 22, no. 9, Jan. 2022, p. 3601.
3. Kim, Jin Su, et al. "A Study on Implementation of Real-Time Intelligent Video Surveillance System Based on Embedded Module." *EURASIP Journal on Image and Video Processing*, vol. 2021, no. 1, Nov. 2021, p. 35. BioMed Central.
4. Yadav, Aniket, et al. *Intruder Detection System: A Literature Review*. 3866777, 7 May 2021. Social Science Research Network.
5. Khan, Khalid, et al. "A Survey on Intrusion Detection and Prevention in Wireless Ad-Hoc Networks." *Journal of Systems Architecture*, vol. 105, no. Complete, 2020. Scholars Portal Journals.
6. Castro, J. L., et al. "Intelligent Surveillance System with Integration of Heterogeneous Information for Intrusion Detection." *Expert Systems with Applications*, vol. 38, no. 9, Sept. 2011, pp. 11182–92. ScienceDirect,
7. Iqbal, Muhammad Javed, et al. "Real-Time Surveillance Using Deep Learning." *Security and Communication Networks*, vol. 2021, Sept. 2021, p. e6184756.