Smart security surveillance system with face and action recognition

Sairaj P. Rajput
sairaj.22111025@viit.ac.in

Tushar V. Kalaskar
tushar.22110965@viit.ac.in

Vilas B. Rabad
vilas.22110883@viit.ac.in

Dr. Pravin Futane
pravin.futane@viit.ac.in

Department of Information Technology,VIIT, Pune

***Abstract*—**

The growth of smart surveillance systems has become necessary in recent years to guarantee the security and safety of different surroundings. This study provides a novel way to machine learning-integrated smart security surveillance using Python and related modules. Action and facial recognition are among the system's primary functions. Convolutional Neural Networks (CNN) are utilized for reliable and effective identification procedures.

Our suggested solution improves performance and accuracy in real-time surveillance scenarios by utilizing the robust machine learning algorithms combined with Python's ecosystem, which includes libraries like TensorFlow, OpenCV, and Keras. The system improves its recognition skills through ongoing learning and adaptation, which helps it recognize intricate movements and recognize people in observed situations.

Additionally, by allowing the system to promptly send alerts and notifications to specific recipients in the event of detected security breaches or suspicious activity, the integration of Twilio API promotes seamless communication. This feature improves the system's ability to respond quickly and effectively to possible security threats.

Keywords: Python, Machine learning, CNN, Twilio API, Open-CV, LBPH, Mediapipe,ANN.

I. INTRODUCTION

In the current scenario, security is an essential aspect of our daily lives. However, many households find traditional security camera systems to be cost-prohibitive. To address this issue, this paper focuses on presenting a solution that is both cost-effective and incorporates facial and action recognition systems.

We propose the introduction of a security surveillance system capable of recognizing both the actions of intruders and the faces of individuals. Upon detection, the system will promptly notify the owner, providing real-time updates on the actions performed by the intruder.

To achieve this, we have developed a dataset and employed technologies such as Mediapipe, CNNs (Convolutional Neural Networks), and other Python modules. Mediapipe is utilized for extracting landmarks from body postures, which are then used to predict the position of individuals.

Our objective is to offer a cost-effective, user-friendly system capable of facial and action recognition, adaptable to various scenarios and environments.

II. LITERATURE SURVEY

Paper	Description	Limitations	Future Scope
1. Enhancing Home Security Using SMS-based Intruder Detection System.	The system described in this paper, uses GSM system for messaging services.For intruder detection this paper implements the hardware components like sensors, Sim900 GRPS /GSM Module.The system is very beneficial for people who want to safeguard their properties and restrict access.	This system has the drawback when there is no network in such situations this system will fail. ii. The system is limited to the area with the GSM network available and the whole system does not work without the network.	i. The SIM900-GPRS module and the microcontroller will be used to communicate between the mobile phone and the devices and sensors installed at home. ii. The mobile phone will be used as a controller from anywhere in the world if the GSM network is available. In addition, three sensors are used as a heat detector, motion detector and intrusion detector which trigger the alarm upon reaching the critical limit.
2.An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients.	The paper introduces a security monitoring system leveraging IoT (Internet of Things) technology. The system comprises Raspberry Pi 3, Arduino, PIR sensor, webcam, and a buzzer. Notably, the novelty of this system lies in its incorporation of human detection capability through the use of the Histogram of Oriented Gradients (HOG) and Support Vector Machine (SVM) methods, with the buzzer serving as a warning mechanism for the homeowner.		The paper suggests that future research will delve into exploring alternative feature extraction and classification methods aimed at further enhancing the accuracy of intruder detection.

3.Real Time Intrusion Detection System Using Opencv.	The study presents a system featuring a Graphical User Interface (GUI) and achieving a remarkable accuracy of 94.5% in face recognition. Initially, users are required to input individual data, allowing the model to undergo training. Subsequently, the system utilizes this data to recognize individuals. It's noted that the accuracy of the system is contingent upon the size and quality of the camera's frame	the accuracy of the system is contingent upon the size and quality of the camera's frame	
4. CCTV Intruder Detection System	This study aims in developing the system which aims in providing the home security surveillance system. The project possesses a distinct advantage in terms of time and efficiency compared to similar systems discussed.	i. A further limitation was lack of computers with sufficient processing power to process continuous streaming of images. ii. The existence of CCTV Camera systems which are not compatible with the Windows and Linux operating systems was another limitation.	i. The scope of the project mainly extends to such areas as image capturing, image processing, and image comparison. ii. The project also covers image enhancement and restoration for improvement of pictorial information. Further, it will include information extraction for further computer analysis.

The system described in this paper, uses GSM system for messaging services.For intruder detection this paper implements the hardware components like sensors,Sim900 GRPS/GSM Module.The system is very beneficial for people who want to safeguard their properties and restrict access. This system is very affordable and easily operated, so that anybody whether rich or comfortable, young or old can make use of this system.But this system has the drawback when there is no network in such situations this system will fail. [1]

The paper introduces a security monitoring system leveraging IoT (Internet of Things)

technology. The system comprises Raspberry Pi 3, Arduino, PIR sensor, webcam, and a buzzer. Notably, the novelty of this system lies in its incorporation of human detection capability through the use of the Histogram of Oriented Gradients (HOG) and Support Vector Machine (SVM) methods, with the buzzer serving as a warning mechanism for the homeowner.

Simulation results demonstrate that the system can swiftly detect intruders within seconds, achieving an accuracy of 90% with a processing time of approximately 2 seconds. The paper suggests that future research will delve into exploring alternative feature extraction and classification methods aimed at further enhancing the accuracy of intruder detection.[2]

The study presents a system featuring a Graphical User Interface (GUI) and achieving a remarkable accuracy of 94.5% in face recognition. Initially, users are required to input individual data, allowing the model to undergo training. Subsequently, the system utilizes this data to recognize individuals. It's noted that the accuracy of the system is contingent upon the size and quality of the camera's frame..[3]

This study aims in developing the system which aims in providing the home security surveillance system. The project possesses a distinct advantage in terms of time and efficiency compared to similar systems discussed. Unlike conventional surveillance systems where all recorded videos must be manually reviewed to identify intrusions, our system offers immediate detection. This is facilitated by the generation of an email for the user, containing vital information such as the time of intrusion and accompanying images. Furthermore, our system is designed to minimize false alarms by adjusting the threshold pixel value of intruder images. Users also benefit from the ability to observe intrusions in real-time through live video, enhancing the overall outcome of the project.[4]

The system outlined in this paper integrates PIR sensors, RFID technology, Arduino microcontrollers, and hazard lights, in addition to OpenCV integration. Specifically, the system utilizes the Haar Cascade Frontal Face Detection algorithm for facial recognition.

This comprehensive system aids in the detection of potential culprits and promptly sends images to the system owners, facilitating immediate action. Its versatility allows for implementation in various settings, including home security and secure locations such as banks and jewelry shops.[5]

The paper describes how the system operates by detecting the motion of intruders through PIR sensors, capturing their images accordingly. Leveraging the Haar Cascade algorithm enhances computational efficiency and accuracy in human face detection and recognition. Remarkably, the system achieves an image processing rate of approximately 28 images per second for the entire process.

Utilizing IoT technology, the system promptly sends alert emails to the owner, containing the latest captured image of the intruder. This low-cost solution proves to be fast, highly accurate, and efficient in providing alerts, effectively serving as a monitoring system. Its convenience makes it adept at addressing security concerns, ultimately contributing to the reduction or prevention of break-ins.[6]

This paper uses ESP32-CAM module which offers a versatile solution for animal intrusion detection, applicable across various sectors. It promises to enhance wildlife preservation, protect agricultural assets, fortify property security, prevent infrastructure damage, and support environmental research. Despite its advantages, such as cost-effectiveness and scalability, addressing limitations like detection range and weather sensitivity is crucial. With careful planning and optimization, this technology can significantly contribute to safeguarding assets and preserving wildlife and ecosystems.[7]

Gaps identified:

1] Cost: In this system we have discovered that most of the systems were expensive due to use of sensors and arduino uno.

2] Video Poor Quality:Poor video quality results in inaccurate predictions.

III. EXISTING SYSTEM

The development of intruder detection systems has been essential in the field of security to protect different settings from possible dangers. To meet the many security needs of contemporary society, a range of technologies and approaches have evolved, from conventional alarm systems to sophisticated smart intrusion detection systems. These solutions are designed to improve overall security posture, provide quick response mechanisms, and provide timely intrusion detection. In order to guide the development of more reliable and effective security measures, it is critical to evaluate and comprehend the capabilities and limitations of current intruder detection systems as technological breakthroughs continue to change the landscape of security solutions.

Let's now move on to describe how the current systems are used.

A. Conventional alarm systems:

Conventional alarm systems, which use sensors like motion detectors, door/window sensors, and glass break detectors, have long been used as a means of detecting intruders. When these systems detect movement or illicit access within a monitored area, they sound an alert or alarm. Although they work well for simple intrusion detection, they could not have sophisticated capabilities like remote access and real-time monitoring.

B. Systems for Video Surveillance:

Conventional alarm systems, which use sensors like motion detectors, door/window sensors, and glass break detectors, have long been used as a means of detecting intruders. When these systems detect movement or illicit access within a monitored area, they sound an alert or alarm. Although they work well for simple intrusion detection, they could not have sophisticated capabilities like remote access and real-time monitoring.

C. Systems of Security Based on IoT:

IoT-based security systems leverage interconnected sensors, cameras, and devices to monitor and secure physical spaces. These systems utilize IoT connectivity to enable remote monitoring and control, allowing users to access surveillance feeds and receive alerts from any internet-connected device. Machine learning algorithms may be employed for anomaly detection and predictive analytics, enhancing the system's ability to detect and respond to security threats in real-time.

D. Biometric Access Control Systems:

Biometric access control systems use distinct biometric identifiers, like fingerprints, face recognition, or iris scans, to confirm people's identities. These systems provide a high degree of accountability and security because biometric data is hard to falsify or duplicate. Organizations can improve security at entrance points and access control mechanisms and guarantee that only authorized personnel are allowed access to secured areas by integrating biometric access control with intruder detection systems.

IV. METHODOLOGY

The proposed system in this research paper comprises three key modules: face recognition, action recognition, and message sending. Operating via the smartphone application IP WEBCAM, the system detects moving objects. Upon detecting an intruder, it utilizes the Twilio API to send a message alert to the owner.

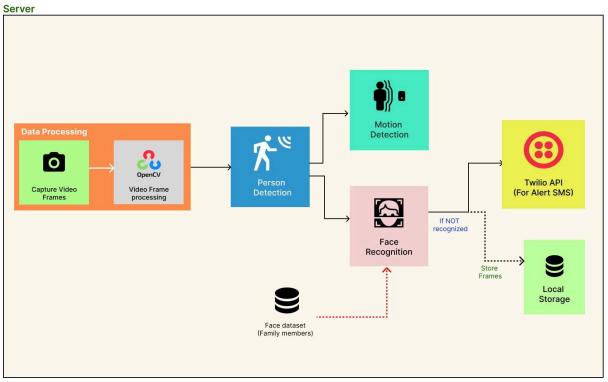

Fig 1: System Architecture Diagram

System workflow

A. Starting server in IP Webcam

Begin by logging into IP WEBCAM, then initiate the server from the application.

B. Get the IP Url from IP Webcam

Retrieve the IP WEBCAM server IP and paste it into the UI Url field, adjusting the camera's position as needed.

C. Video Processing

Observe live video footage processing. The motion detector algorithm detects any invasion by utilizing the MOG2 algorithm for background subtraction, enabling the detection of moving objects against a static background.

D. Face recognition

Upon detecting a moving person, the system crops the area around them and tracks their coordinates. Utilizing the Haar cascade algorithm for face detection and a CNN model for recognition, the system identifies the person. If authorized, it sends a message regarding the activity to the authorized individual.

E. Action recognition

The system obtains landmarks of the person, representing the coordinates of each body part. Based on these coordinates, it predicts the person's position.

F. Sending message

Finally, the system saves frames where intruders are detected and sends a message to the system owner.

This system uses 2 deep learning algorithms:

Action Recognition Model:

An artificial neural network (ANN) is an algorithm that mimics the human brain. Artificial Neural Networks contain artificial neurons, which are called units. These units are arranged in layers, constituting the entire artificial neural network in the system. Commonly, the artificial neural network will have one input layer, one middle layer, and a third output layer, with a hidden layer between them. The input layer accepts data from the outside world, the hidden layer preprocesses the data, and the output layer provides the response in the form of response data. Each of these connections has weights that determine the influence of one unit on another unit. As the data transfers from one unit to another, the neural network learns more about the data, eventually resulting in an output from the output layer.

The proposed system utilizes the ANN Algorithm for predicting the position of a person using landmarks.

The following steps are taken for constructing the action recognition model based on the ANN Algorithm:

1. Creation of the dataset: A total of 200 images are collected for running, standing, walking, and waving activities. These images are split into 75% for training and 25% for testing purposes.

2. Generation of CSV File: The coordinates of each part of the training data are generated using the mediapipe library, and each class registers the coordinates. The model

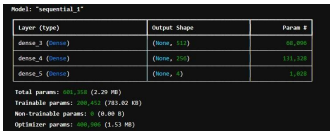

Fig. 2.Action Model Summary

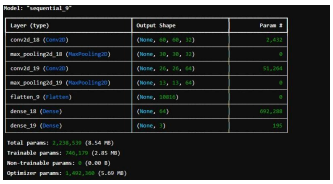

Fig. 3.Face-model Summary

is then trained based on the CSV file.

3. Creation of the ANN Model and training: The ANN model is created and trained based on the CSV file data.

Face Recognition Model:

A Convolutional Neural Network (CNN) is a specialized type of artificial neural network commonly used for tasks like image recognition, including face recognition. CNNs consist of multiple layers, including convolutional layers, pooling layers, and fully connected layers. These networks automatically learn spatial hierarchies of features from input images. In face recognition, CNNs analyze facial features at different levels of abstraction, enabling accurate and reliable face recognition. Despite facing challenges in predicting unauthorized individuals, a secondary model based on the LBWH algorithm of OpenCV is trained to address this issue.

1. Creation of the dataset: A total of 150 images of 4 persons are collected and split into 70% for training and 30% for testing. These images are converted into grayscale images of size 64 by 64.

2. Creation and training of the CNN Model: The CNN model is created and trained on the dataset achieving an accuracy of 94.03% with 12 epochs.

3. LBPH Model: A model based on the LBWH algorithm is trained on the same dataset.

4. Saving: Both models are saved in separate directories.

5. Loading the models: First, the confidence value predicted by the LBPH-based model is obtained. If the value is greater than 85, the person is unrecognized, and the second model is not used. Otherwise, if the value is less than 85, the person is recognized, and their face can be predicted.

Saving detected Frames:

This system makes use of a max heap data structure, which holds timestamps, frames, and the percentage change relative to the base frame. Elements are arranged in the heap according to the largest percentage difference between the current frame and the base frame. The motion detection MOG2 algorithm is used by the camera to recognize the presence of a person when they enter its field of view. After drawing a box around the moving object, the system saves the frame along with the relative percentage change from the base frame. The top 30 frames from the maximum heap will be saved when a player exits the field.

V. RESULT

A. Action Recognition Model:

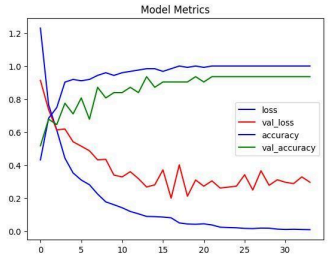

Fig. 4.Metrics

The action recognition model achieved the accuracy of 93.00% accuracy and testing accuracy of 93.07%.The model trained with 200 epochs, 16 batch size.

Fig. 5.Testing on sample

B. Face Recognition Model:

The CNN model achieves the accuracy of 94.04%.this model trained on 105 images and 45 images in 70% and 30%.

Fig. 6.Testing of face recognition model

C. Message Sending API:

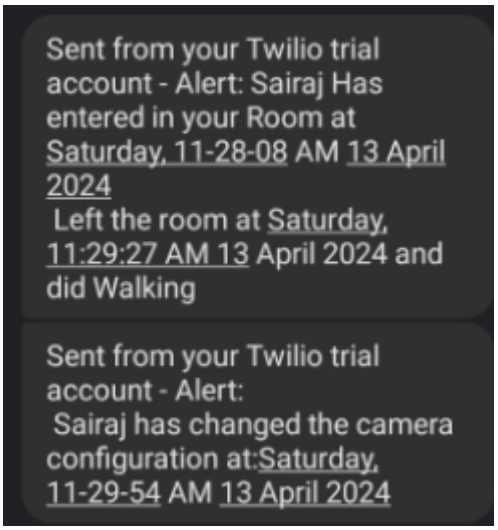

Fig. 7 Message sending API Testing

This system uses Twilio API for sending messages regarding changes in camera configuration and changes in base frame.

VI. CONCLUSIONS

The proposed system integrates face recognition, action recognition, and message sending modules, operating through the IP WEBCAM smartphone application. Leveraging artificial neural networks (ANN) for action recognition and convolutional neural networks (CNN) for face recognition, the system achieves impressive accuracies of 93.00% and 94.04%, respectively. By efficiently detecting intruders and sending timely alerts via the Twilio API, the system enhances security measures in diverse settings. With its robust performance and streamlined workflow, the system holds promise for effective deployment and widespread adoption.

VII. REFERENCES

[1] Nwalozie G. C, Aniedu A. N, Nwokoye C. S, Abazuonu I.E.Department of Electronic and Computer Engineering, Nnamdi Azikiwe University Awka, Anambra
State
Enhancing Home Security Using SMS-based Intruder Detection System

[2] Nico Surantha and Wingky R. Wicaksono.
Department of Computer Science, BINUS Graduate Program Master of Computer Science,Bina Nusantara University, Jl. Kebon Jeruk Raya No 27, Jakarta 11480, Indonesia. An IoT based House Intruder Detection and Alert System using Histogram of Oriented Gradients

[3] Akula Surya Teja, Ginni Chandra Mohini,Dannana Dhanunjay, Dr P M Manohar Students, Dept. of
Computer Science and Engineering, Raghu Engineering College,Visakhapatnam Real Time Intrusion Detection System Using Opencv.

[4] G.H.A.Chaminda, University of Colombo School of Computing 2019. CCTV Intruder Detection System

[5] MVD Prasad,N. Sai Kiran,Ch Sumanth,T V V R N Sri Harsha, Sk Hasane Ahammad, Department of ECE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India-5222502.Video surveillance-based security system using OpenCV and Arduino uno

[6] G.Mallikharjuna Raoa, Haseena Palleb, Pragna Dasaric, Shivani Jannaikode. Implementation of Low Cost IoT Based Intruder Detection System by Face Recognition using Machine Learning.

[7] Pradeep S, Nikhil Raghav V, Bharath Kumar S P,Department of Electronics Engineering Bannari Amman Institute of Technology Sathy, Tamil Nadu. Animal Intrusion Detection Using ESP32 Cam and OpenCV[2023], [8]