Realtime Intrusion Detection System Using Open CV

[1]Akula Surya Teja, [2]Ginni Chandra Mohini, [3]Dannana Dhanunjay, [4*] Dr P M Manohar

[1,2,3] 4th B.Tech Students, Dept. of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam

[4] Associate Professor, Dept. of Computer Science and Engineering, Raghu Engineering College, Visakhapatnam

manohar.pattisapu@raghuenggcollege.in, 19981a0503@raghuenggcollege.in, 19981a0552@raghuenggcollege.in, 19981a0537@raghuenggcollege.in

Abstract

Security in restricted areas is essential for protecting valuable assets, sensitive information, ensuring the safety of personnel from intruders. Traditional security systems have many limitations, where they cannot authenticate whether the entered person is an intruder or not. Authentication of the entered person can be done by face identification, through which a smart security system can be developed. Creating and implementing a face recognition-based surveillance system is the goal of this project. Realtime Intrusion detection system provides surveillance for restricted and confidential areas with help of face recognition and detection, when an intruder or unauthorized person enters the area, this system will give an alert to the respective in charge or buzzer an intrusion alarm. Facial recognition is a method of recognising an individual. In this system, the OpenCV python library along with several algorithms are used to abstract the facial features and to take the input dataset. For face recognition, LBPH algorithm is used. With help of this technique, we can ensure whether the entered person is an intruder or an authorized one. Accuracy of the face recognition is 94.5%. A GUI (graphical user interface) is developed for ease of accessibility with the help of python tkinter.

Keywords: Intrusion, face recognition, Local Binary Pattern Histogram, python, tkinter

1.INTRODUCTION

Security concerns in confidential or restricted areas are of paramount importance as they involve protecting sensitive information, assets, and personnel from unauthorized access, theft, sabotage, or espionage. These areas may include government facilities, corporate offices, research labs, financial institutions, and data centers, among others. In some areas like government or nuclear facilities, every department requires unique protocols for accessing, only a particular set of authorized persons should have entry, and in other cases, entry of every person into the particular department should be monitored.

There have been many options in both biometric and traditional technologies over the recent past to fulfil the requirements for homes' or businesses' security Certain standard security mechanisms, such as those involving credentials, passwords, Identity cards, and/or RFID cards, may not be reliable if objects needed for access are stolen or lost. [2]. Conventional security systems cost a lot of money and have few sophisticated features like real-time detection, immediate alerts, and rapid reporting [12].

This can be overcome by the authentication of every individual Authentication is one of the largest issues facing information systems today.. One of the recognised methods for user authentication includes, among other things, the ability to recognise a human face [1].

The state of surveillance cameras today has shown that there is still a great deal of potential for development in the fundamental ways that they work. Security cameras have always been employed as a monitoring system, even if they have never been used as an intrusion detecting and warning system. Surveillance cameras are worthless when used

to merely monitor a single space, but if we can leverage the current technology to incorporate facial recognition, we can increase the level of security in our homes and workplaces [6].

2.LITERATURE REVIEW

Intruder detection systems for security and surveillance systems are widely used today. They require either a long installation process or human assistance to identify an intruder, and there is a possibility that alerts could also occur.

G.Mallikharjuna Rao et al. say, The USB Camera is triggered by a PIR sensor to take a picture of the person. Using OpenCV and machine learning methods, faces are detected and identified. Raspberry Pi compares the authorized photos stored in the database with the detected face. Regardless of whether the person is authorized or not, it emails the owner. [5]

The system implemented by Bazama A et al. consists of two parts: a camera and software required for face detection and facial recognition. The Viola-Jones method was employed for recognizing the face, and face identification was performed out by using MATLAB's independent component analysis (ICA). Accuracy:86.7% [1]

A system developed by S. Menaga et al. employs a PIR sensor to identify human motion, which the Pi camera then records. Once the retrieved face has been identified, an HDMI cable is used to transfer it to the Raspberry Pi. Open CV Python is used to run this system. When an intrusion happens, the system uses Wi-Fi technology to email the identified image to owner [3].

The purpose of the project created by Dr. Savitha Choudhary et al. is to improve the video surveillance environment using embedded computer recognition technologies. They used the Raspberry Pi 4 and computer vision algorithms like motion detection, image recognition, face identification, etc. to select the region of interest from the recorded video. [12].

The Intrusion Detection System (IDS) that is implemented by the system created by Mfundo Zuma et al. employing a controller and stations at a home setting powered by a Raspberry Pi processor. The system's central processing unit is decided to be the Raspberry Pi 4, which controls all communication between all connected components (such as a passive infrared sensor, web camera, and light emitting diode). The Telegram bot's API is used to integrate the intelligent gadget with it. A notification system and instant messenger generator are both implemented using the API with the necessary Telegram framework [11].

This work by Arnab Pushilal et al. discusses the creation and development of a home surveillance system that employs face recognition to verify the identity of the visitor and implements different safety precautions when unauthorised individuals attempt to access the door. It shows how Principal Component Analysis, one of the most popular facial recognition algorithms, may be used for secure door access. A large number of training data may be collected since PCA reduces the dimensions of the images without sacrificing the key features. The door will open if the face is identified as a familiar one; otherwise, the Arduino Uno microcontroller will classify the face as unknown and instruct the buzzer to begin ringing [10].

3.PROPOSED APPROACH

Deploying a smart surveillance system in restricted areas, which has the ability of face recognition and detection along with the alerting mechanism is the proposed solution for intrusion detection. The approach for the proposed approach consists of 5 stages:

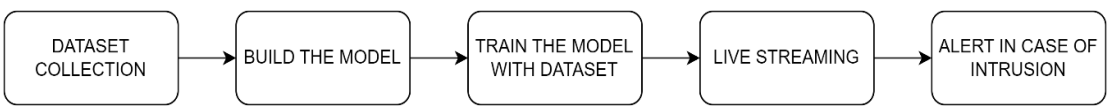


Figure 1 The architecture of the Proposed System

The Haar-Cascade algorithm for dataset collection includes identifying faces of persons, which uses the Local Binary Pattern Algorithm (LBP) for face detection and the Python programming language to organise itself in Open CV. This classifier outperforms other popular algorithms in terms of recognition rate, feature selection efficiency, and even with varied phrases. [8]. For face identification purposes, the Convolutional neural networks are not preferred over the local binary pattern histograms technique [7]. by considering many factors. In order to train the model, the dataset's gathered photos need to go through pre-processing steps including scaling and grayscale conversion. To use the developed system easily, a graphical user interface (GUI) should be required, which can be developed using tkinter.

4.METHOD

Flow chart:

The flow of steps in the process or algorithm of the intrusion detection system can be seen in Figure 2. Through this we can easily understand the sequence of steps involved in a process and make informed decisions based on the information presented.

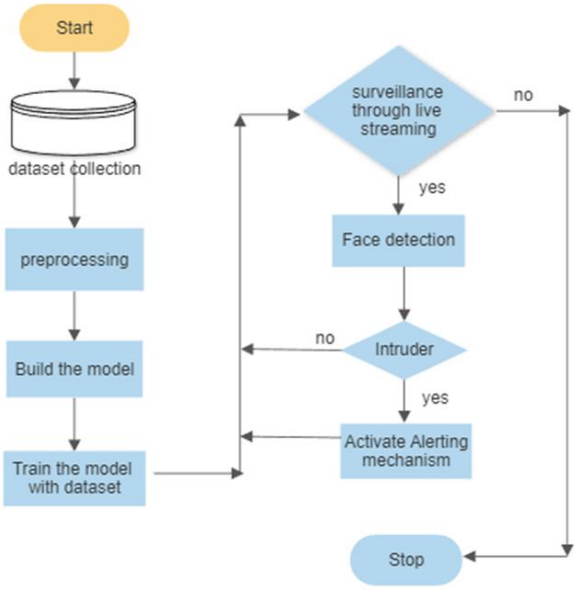
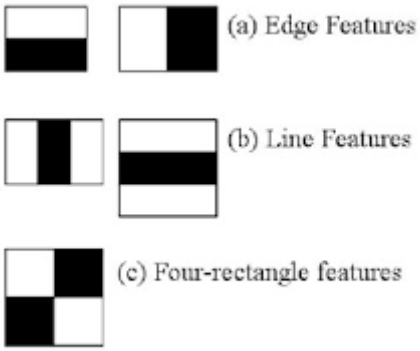


Figure 2 Flow chart of the proposed system

Step1- Dataset Collection: The dataset contains the images of all the authorized users in individual folders. The collection of the images can be done by OpenCV in python. The face of a person is extracted by the Haar-Cascade algorithm.

Haar Cascade algorithm:

With the help of this algorithm, faces can be located in still images or real-time recordings. Even though it's an outdated framework, it's excellent for instant facial recognition. This approach is quite quick in detecting real-time faces, despite the fact that training takes some time. A Haar feature is required for calculations on adjacent centroids at a certain location in a bounding box. Each region's pixel intensities are added, and the variations between the sums are computed.



Step2- Pre-processing: Processing the dataset includes the formatting of collected images into the required size and converting them from colour to Bgr2gray.

Step3- Build the model: Building the model includes loading the classifier for face recognition with help of the LBPH algorithm

LBPH Algorithm:

The LBPH algorithm works by first dividing the image into small, overlapping regions. Then, a binary code is created for each pixel in each region depending on its intensity in relation to the pixels around it. The result is a feature vector for each region, which is created by combining these binary codes. In order to identify the subject of the image, all of the feature vectors for the various areas of the image are eventually integrated into a single feature vector. This is accomplished by comparing the input image's feature vector with a database of feature vectors for identified faces.

$$LBP(gp_x, gp_y) \sum_{p=0}^{P-1} S(gp - gc) \times 2^p$$

$$s(x) = \begin{cases} 1 & if \quad x \geq 0 \\ 0 & if \quad x < 0. \end{cases}$$

gc- Intensity of the central pixel

gp- Intensity of neighbour pixel of index p

P- total number of neighbours on a length of radius R

R- spatial resolution of the method or operator.

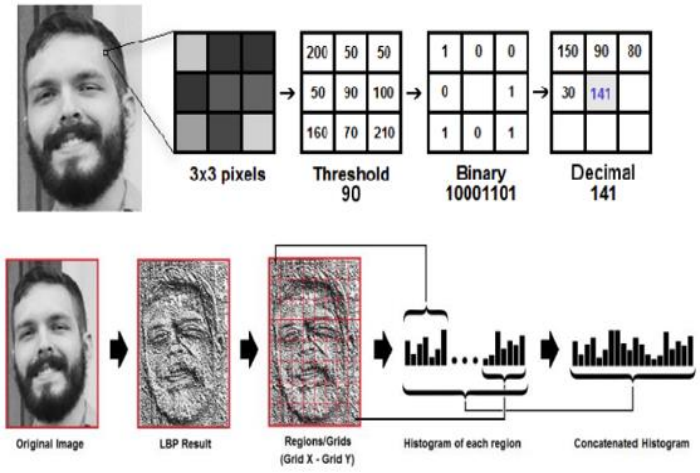


Figure 3 LBPH Image to Histogram Conversion

Step4- Train the model with the dataset: The model should be trained once using the collected dataset which contains all the images of authorized users

Step5- Surveillance through live streaming: The surveillance camera should be deployed in the restricted area for security, Then the area will be under the surveillance of an Intruder detection system

Step6- Intrusion detection: Any person who enters the restricted area will be identified by face recognition and detection using the developed model, through which the person can be differentiated as intruder or authorized.

Step7- Activate Alerting mechanism: If the entered person is an intruder, then immediately alarm or a buzzer should be blown and the intruder's face will be captured.

5.RESULTS AND DISCUSSION

GUI :

GUI that is created for the intrusion detection system, which consists of several functionalities is in below Figure 4

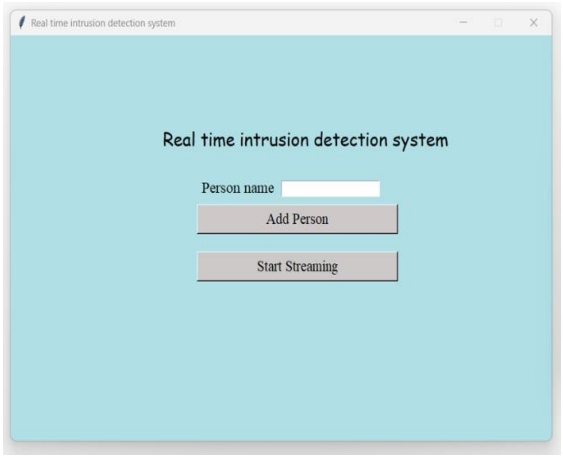


Figure 4 GUI of Real time intrusion detection system

Dataset collection:

Facial images of the authorized users can be can be collected by simply entering the name and all the authorized persons data is stored in folder named dataset as shown in Figure 5.

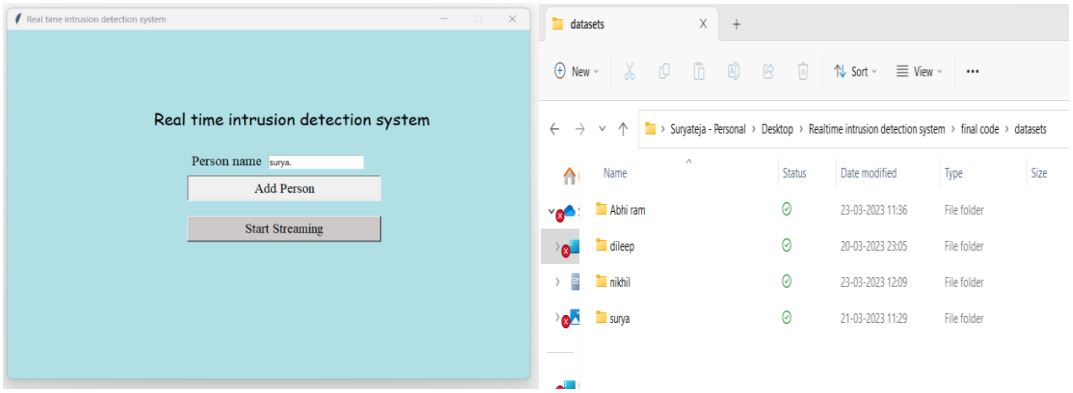


Figure 5 Dataset Collection

Pre-processing:

Pre-processing will be done during the capturing of the faces for dataset as shown in Figure 6.

Figure 6 pre-processed images

Output:

Case 1: Identification of authorized persons: when an authorized person enters the surveillance area, then the name of the person will be displayed on the screen. Even multiple persons' faces can be identified.

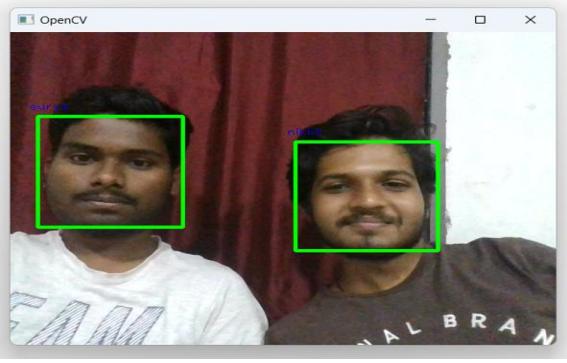


Figure 7 multiple authorized persons

Case 2: Identification of Intruder: when an intruder enters the surveillance area, then the picture of that person will be captured and saved in the intruder's folder along with the date and time of intrusion. And immediately alerts the owner with an alarming sound.

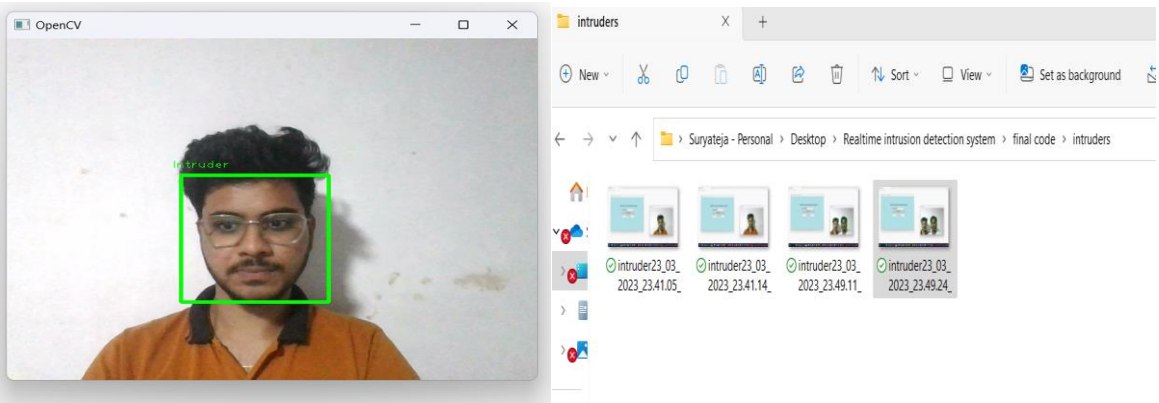


Figure 8 capturing of the intruder's picture

Confidence value vs distance graph

Confidence value: The confidence value represents the distance from the detected face to the closest face in the dataset. Which means a lower confidence value refers to accurate recognition. Distance: The distance in the graph represents the length between the camera and the person in centimeters. It is observed that when the person is nearer to the camera recognition rate is accurate comparatively. And it depends on the quality of the camera used, brightness, and atmospheric conditions.

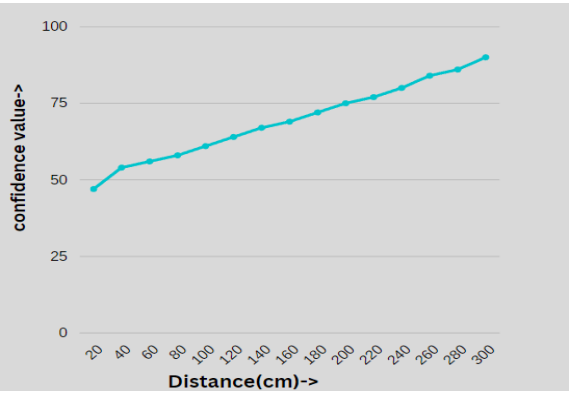


Figure 9 Confidence value vs distance

Accuracy

To calculate the accuracy of face recognition in the developed model, we have collect 200 facial images of different authorized and unauthorized persons.

Accuracy = ((number of facial images considered - number of false recognition)/(number of facial images considered)) X 100%.

For the considered 200 facial images, model recognized 189 images correctly, through which we can say that the accuracy of face recognition in the developed model is 94.5%.

6.CONCLUSION

This project provides an application with a user-friendly graphical user interface (GUI). Where the user can add authorized persons, train the model and start the surveillance. The system implementation also requires a few resources. The accuracy of face recognition is 94.5%, it depends on the size and quality of the dataset provided and also on the quality of the surveillance camera used. In further, intrusion detection systems can be implemented using different algorithms from

deep learning to increase accuracy and it can be developed as a web application.

References

[1] Bazama A, Mansur F, Alsharef N. Security System by Face Recognition. Alq J Med App Sci.2021;4(2):58-67. http://doi.org/10.5281/zenodo.4917446

[2] Nourman S. Irjanto , Nico Surantha. Home Security System with Face Recognition based on Convolutional Neural Network. (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 11, 2020

[3] S. Menaga, A. Priyadharshini , V. Subalakshmi , J. Priyadharshini , P. Velammal . A Smart Intruder Detection System. International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181

[4] Kajenthani Kanthaseelan ,Paskaran Pirashaanthan ,Jasmin Jelaxshana ,Akshaya Sivaramakrishnan,Kavinga Yapa Abeywardena ,Tharika Munasinghe. CCTV Intelligent Surveillance on Intruder Detection. International Journal of Computer Applications (0975 – 8887) Volume 174 – No. 14

[5] G.Mallikharjuna Rao, Haseena Palle, Pragna Dasari , Shivani Jannaikode. Implementation of Low Cost IoT Based Intruder Detection System by Face Recognition using Machine Learning. Turkish Journal of Computer and Mathematics Education Vol.12 No.13(2021), 353-362

[6] Prakash, R., Chithaluru, P. (2021). Active Security by Implementing Intrusion Detection and Facial Recognition. In: Nath, V., Mandal, J. (eds) Nanoelectronics, Circuits and Communication Systems. Lecture Notes in Electrical Engineering, vol 692. Springer, Singapore. https://doi.org/10.1007/978-981-15-7486-3_1

[7] T. Sanjay , W.Deva Priya . Efficient System for Criminal Face Detection Technique on Innovative Facial Features To Improve Accuracy Using LBPH In Comparison With CNN Journal of Pharmaceutical Negative Results, Volume 13, Special Issue 4 ,2022, DOI: 10.47750/pnr.2022.13.S03.085 DOI: 10.47750/pnr.2022.13.S03.085

[8] Md Manjurul Ahsan, Yueqing Li, Jing Zhang, Md Tanvir Ahad , Kishor Datta Gupta Evaluating the Performance of Eigenface, Fisherface, and Local Binary Pattern Histogram-Based Facial Recognition Methods under Various Weather Conditions Technologies 2021, 9, 31. https://doi.org/10.3390/technologies9020031

[9] S. Kasar, V. Kshirsagar, S. Bokan, N. Rathod Smart Physical Intruder Detection System for Highly Sensitive Area.Smart Trends in Computing and Communications, Smart Innovation, Systems and Technologies 165 (2020).https://doi.org/10.1007/978-981-15-0077-0_23

[10] Arnab Pushilal , Sulakshana Chakraborty , Raunak Singhania , P. Mahalakshmi, Implementation of Facial Recognition for Home Security Systems, International Journal of Engineering & Technology, 7 (4.10) (2018) 55-58

[11] Mfundo Zuma, Pius A Owolawi, Vusi Malele, Kehinde Odeyemi, Gbolahan Aiyetoro, Joseph S. Ojo . Intrusion Detection System using Raspberry Pi and Telegram Integration. icARTi '21, 2021. https://doi.org/10.1145/3487923.3487928

[12] Dr. Savitha Choudhary, Ajith D R, H Likith Sai Varma, Lakshman Kumar S, Lekhith R," SMART SURVEILLANCE MONITORING SYSTEM USING MACHINE LEARNING AND RASPBERRY PI", International Research Journal of Modernization in Engineering Technology and Science, Volume:04,Issue:02, 2022

[13] Fahima Tabassum , Md. Imdadul Islam , Risala Tasin Khan , M.R. Amin, Human face recognition with combination of DWT and machine learning, Journal of King Saud University – Computer and Information Sciences 34 (2022

)