

Design and Development of Monitoring and Self-Intrusion System



Achuthakannan A, V Chentala, Siddharth Chander, DG. Y. Rajaa Vikhram

Abstract: Let's talk about security at a private access place taking into account the amount of effort one wants to keep it as such only listed personnel to enter, but intrusions are found, and raising security and scanning alone doesn't bring down one such issue. These days we find that most of the research has a much higher usage of servers which is termed expensive as to run the processing of the software. Few places would not be able to afford such costs. The objective of this project is to provide a surveillance and a self-monitoring intrusion system that ensures regular checking, from the current surveillance of a security personnel. This software aims to classify the people entering and leaving a particular place with a whitelist. This will also help exercise caution that can be implemented in places that require inspection. This system is programmed to alert real-time intrusion to the owner and/or security via MMS. We want to make sure to build a prototype that can sustain such parameters and be market-ready. The core theme of the project is to have another set of surveillance integration to warn/alert the respected person about an intrusion per se someone who's not in the whitelist mentioned.

Keywords: CNN, Deep Learning for training, Raspberry p, Twilio, Adafruit Servo Driver.

I. INTRODUCTION

Well when we talk about intrusion and monitoring, let us just understand the act of this kind which is being systematically set up at almost every place nowadays, whether small or relevant or even necessary. Hence we see a need for this system to be integrated everywhere. A monitoring system is a base for surveillance as it is constantly on the watch and we would want it to be able to classify the persons who are entering and leaving and to detect when someone in the field of view of the installed camera. A security system is a method in which something important is secured with the interconnected components and networks. Security systems are implemented at commercial as well as residential areas, a popular example being surveillance cameras(CCTV), but they are only used whenever there is a need to go back and trace an incident such as an act of burglary, for example. Although there is a human presence to avoid such

circumstances, even he/she is bound to make errors sometimes in detecting a person coming and going. This system aims to reduce such incidents by entering a dataset of people who have access to a particular area and alert to the mobile phone of the concerned person. This will give a time stamp and photo of the frame as the software deems it as an unrecognizable or unknown person.

II. PROPOSED METHOD

A. Gathering Dataset

Here we first start by gathering a dataset i.e. we take a picture of the whitelist person that has permission or access to enter and leave the premises in check. The major advantage of the method we propose here is that we only require a single good quality picture of a person in any image reading format to be able to recognize the person when he enters the frame. This saves a lot of time as we don't have to build a wide range of datasets with multiple frames about a single person, and it is able to detect the face efficiently when it is in the field of view of the camera.

B. Face Recognition and Alert

Code for training the face is integrated alongside the recognizer code. We only run once with the dataset imported on the folder. A localizer[5] is a function that detects the facial features of a person. When the camera starts capturing frame by frame, the captured frames are sent to OpenCV which uses the facial recognition method and haar cascade to compare with the dataset. When there is a match[Fig. 1.], it means that the person is guaranteed access and no intrusion message is alerted, and during a mismatch[Fig. 2.], there is an intrusion that triggers an alert message to the users mobile in the form of MMS. TWILIO[4] handles the cloud computing platform services for such an alert task.

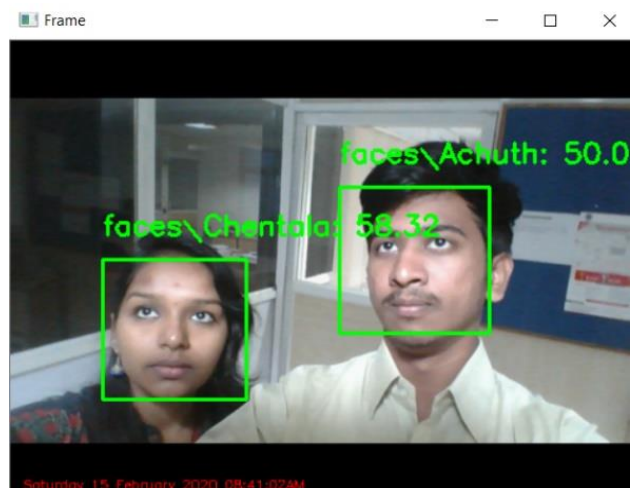


Fig. 1. Identification of known faces.

Revised Manuscript Received on April 25, 2020.

* Correspondence Author

Achuthakannan A*, B.Tech EIE, SRM Institute of Science and Technology, Chengalpattu, India. Email: achuthakanna@gmail.com

V Chentala, B.Tech EIE, SRM Institute of Science and Technology, Chengalpattu, India. Email: chentala.v@gmail.com

Siddharth Chander, B.Tech EIE, SRM Institute of Science and Technology, Chengalpattu, India. Email: siddharthchander98@gmail.com

Dr. G. Y. Rajaa Vikhram, Assistant. Prof. of EIE dept., SRM Institute of Science and Technology, Chengalpattu, India. Email: raajaviy@srmist.edu.in

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

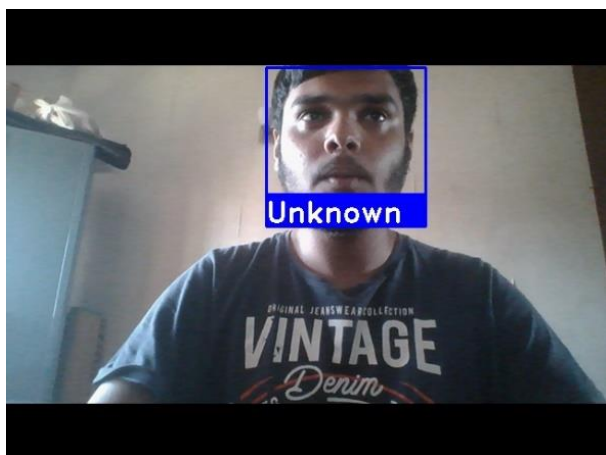


Fig. 2. Frame localizing unrecognized face.

C. Hardware Setup

This is to provide a working feature of the algorithm code and camera functionality. To gather wide ranges of view for the camera to not miss the facial features of a person at its line of sight, we provide a camera pan/tilt[7][Fig. 3.]. This provides the camera with a turn of 180 degrees vertical and 180 degrees horizontal. For this purpose, we use an Adafruit Servo Driver board for driving the servo motors better than to use the Raspberry pi directly.



Fig. 3. Hardware setup

III. ALGORITHM

The advantage of this proposed method is the pre-trained algorithm- is good at detecting faces. The Haar cascades notice the facial features and start capturing it frame by frame. These frames are then sent to the Machine Learning algorithm which has the capability to predict and produce results. The algorithm used here for image classification is the Convolutional Neural Network or CNN. The CNN remembers the features of the image and then detects and recognizes them using deep neural nets.

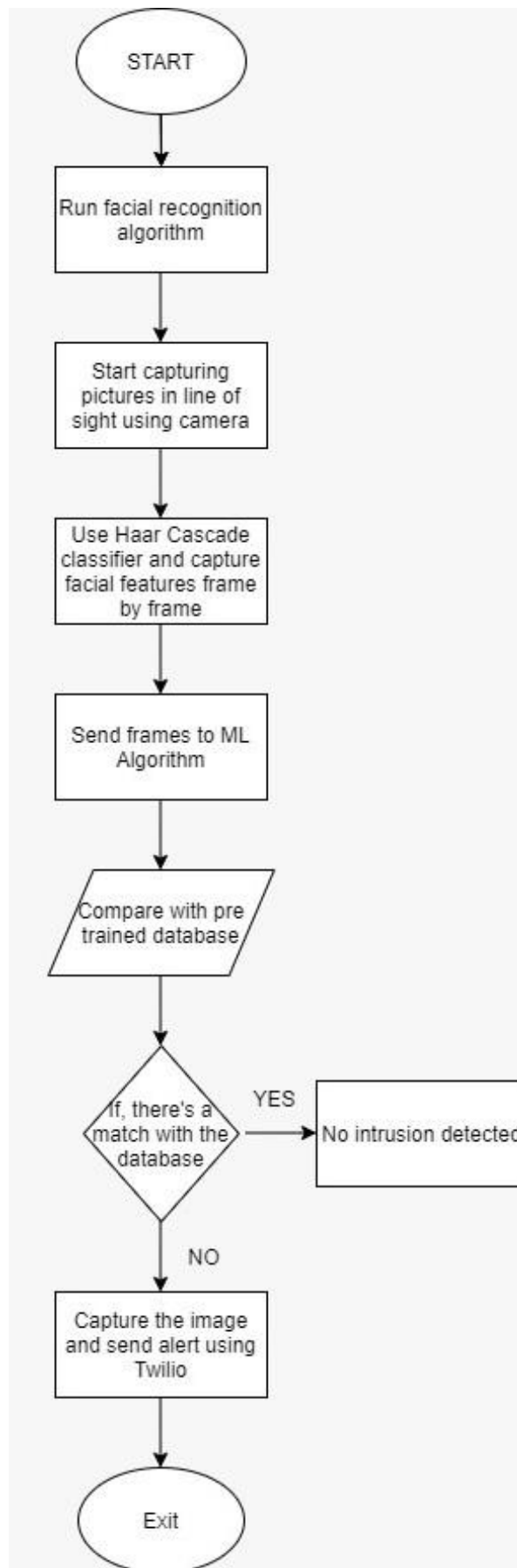


Fig. 4. Architecture flowchart

IV. ARCHITECTURE

Architecture comes with the software and the hardware components. The software part includes a GTX 1050 powered computer to run the Dlib’s face recognition built with deep learning neural nets. The input images or the images in the database are then classified as faces using the Haar cascade. It requires Python 3.3 or Python 2.7 to use the libraries with the other python libraries for face recognition.

The command line “face_recognition” and “face_detection” do all the essential work.

Now, coming to the hardware part, it has a Raspberry Pi along with a Pi camera to capture the live feed, a pan-tilt mechanism which provides a 0 to 180-degree movement using the servo motors. This allows face tracking which can try to locate the facial features and move the camera accordingly with the help of this setup mechanism.

As the name suggests, face_detection gets all the facial features and face_recognition for comparing the pictures to study whether there is a match or not. The image in the database (folder) is compared with the real-time image as seen in the camera and the algorithm can predict whether it is a known or an unknown face.

Twilio is an API that is used to send personalized messages. Since our prototype requires real-time alerts few use Twilio with AWS(Amazon Web services) platform for the same. Here the AWS is the clouding platform to store the picture sent from the camera of the intruder detected.

This now authorizes a user access key to implement a secure procedure to send the pic only to the registered device we set. The API platform is also python friendly as we can use this to access the Twilio API from the libraries.

V. RESULT

The program is executed, the camera localizes the facial features of a person under the frame and gives a boxed frame outcome with the name of the person from the whitelist entered into the database. If an unknown person is detected, i.e. one whose database is not entered, the boxed frame will turn red and we’ll receive an alert in our mobile through MMS[Fig. 5.].

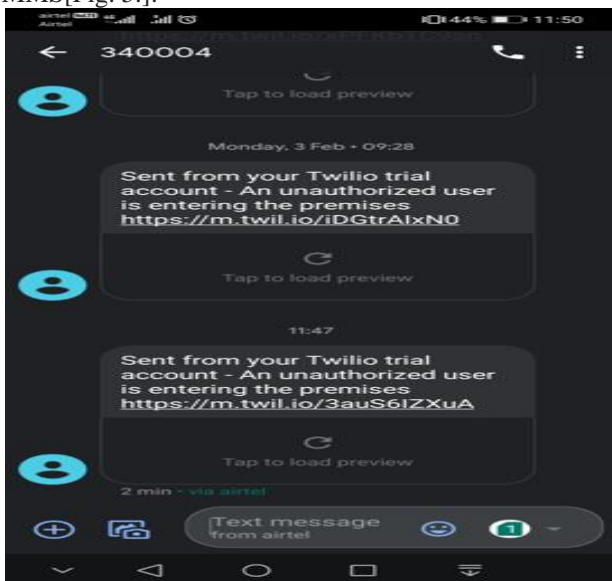


Fig. 5. Alert messaged received when an intruder is detected.

VI. CONCLUSION

The prototype of the design and development of monitoring and intrusion system using deep learning neural nets facial recognition is implemented and tested. As the paper suggests, the system is able to classify a person as a known or an unknown person with the help of the given input images on the database and can send an alert to the concerned person. The usage of Raspberry Pi[8], Python using OpenCV and the pan-tilt mechanism helps to create a low cost yet effective intrusion detection for real-time purposes. For example, a storeroom. With a better algorithm and supporting hardware and software components, this can be implemented for large scale purposes, say, crowded places like shopping malls.

REFERENCES

1. Khirod Chandra Sahoo, Umesh Chandra Pati, "IoT Based Intrusion Detection System Using PIR Sensor", 2017, IEEE RTEICT (International Conference on Recent Trends in Electronics, Information & Communication Technology), pp.1641-1645.
2. Rutvik Kakadiya, Reuel Lemos, Sebin Mangalan, Meghna Pillai, Sneha Nikram, "AI-Based Automatic Robbery/Theft Detection Using Smart Surveillance in Banks", 2019, ICECA (International conference on Electronics, Communication and Aerospace technology), pp.201-204.
3. M. Sathishkumar, S. Rajini, " Smart Surveillance System using PIR Sensor Network and Gsm", 2015, IJAR CET(International Journal of Advanced Research in Computer & Technology), Vol. 4, Issue 1, pp.70-74.
4. S.Varsha, N.Roshne, " Design And Implementation Of An Automated Security System Using Twilio Messaging Service", 2017, ICON-SONICS (International Conference on Smart Cities, Automation & Intelligent Computing Systems), pp.59-63.
5. Jin-Xiang Wang, " Research And Implementation Of Intrusion Detection Algorithm In Video Surveillance", 2016, ICALIP (International Conference on Audio, Language and Image Processing), pp.345-348,
6. Chandan N Bhagwat, Y. Navaneeth Krishnan, K Badrinath, " Cloud-Based Intruder Detection System", 2015, ICECS (International Conference on Electronics and Communication Systems) pp.1244-1246.
7. Hongkai Chen, Xiaoguang Zhao, Min Tan "A Novel Pan-Tilt Camera Control Approach for Visual Tracking", 2014, IEEE, pp.2860-2865.
8. Yellanti Venkat Vivek, P Chandhan, Praneeth Komati "Intruder Detection Using Face Recognition and I.O.T services on Raspberry Pi", 2018, IJRASET (International Journal For Research in Applied Science and Engineering Technology), pp.22-26.
9. Prof.Rakhi Bharadwaj, Kiran Bera, Onkar Jadhav, Prachi Gaikwad, Tamanna Gupta "Intrusion Detection through Image Processing and getting Notified Via SMS and Live Streaming", 2018, IRJET (International Research Journal of Engineering and Technology), Vol. 5, Issue 12, pp.683-686.
10. Kalathiripi Rambabu, V.Haritha, S.Nikhil Srinivas, P.Sanjana Reddy, "IoT Based Human Intrusion Detection System using LabView", 2019, IJITEE (International Journal of Innovative Technology and Exploring Engineering), Vol. 8, Issue 6S4, pp.557-560.

AUTHORS PROFILE



Achuthakannan A became a member of IET in 2016. Achuthakannan was born in Chennai, Tamilnadu, India. He is currently pursuing Bachelor’s Degree B.Tech in the stream of Electronics and Instrumentation from SRM Institute of Science and Technology, Chengalpattu, India.



Chentala V became a member of IET in 2016. Chentala was born in Karur, Tamilnadu, India. She is currently pursuing Bachelor's Degree B.Tech in the stream of Electronics and Instrumentation from SRM Institute of Science and Technology, Chengalpattu, India. She has also participated in a national level hackathon, Smart India Hackathon.



Siddharth Chander became a member of IET in 2016. Achuthakannan was born in Chennai, Tamilnadu, India. He is currently pursuing Bachelor's Degree B.Tech in the stream of Electronics and Instrumentation from SRM Institute of Science and Technology, Chengalpattu, India.



Dr. G. Y. Rajaa Vikhram is working as Assistant Professor at the Department of Electronics and Instrumentation Engineering, SRM IST. He has completed his Bachelor's degree in Electrical and Electronics Engineering from K.L.N. College of Engineering in 2009 and a Master's degree in Control and Instrumentation from Thiagarajar College of Engineering, Madurai in 2011. He also got his doctorate in Electrical and Electronics Engineering from Thiagarajar College of Engineering, Madurai in 2017. He has published various papers on the topic of Power System Control. He has also received the Best Outgoing Student award for M.Tech (Control & Instrumentation) in Thiagarajar College of Engineering, Madurai for the year 2011.