



iJRASET

International Journal For Research in
Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 Issue: VII Month of publication: July 2021

DOI: <https://doi.org/10.22214/ijraset.2021.36758>

www.ijraset.com

Call:  08813907089

E-mail ID: ijraset@gmail.com

Smart Security System Using Image Recognition

Arpita Prakash Hegde¹, Neha Pawar K R², Nidhi S Jain³, Nikita B N⁴, Yashaswini Bandloor V⁴, Naseer R⁵

^{1, 2, 3, 4, 5} Department Computer Science and Engineering, BIET Davanagere

Abstract: *The Smart Security System using Image Recognition uses Deep Learning and Computer Vision approach. In real time it would help the home based security system to track the persons coming into the house and unlocking the door, hereby the system would be accessed by using the image recognition service in which the images are trained in different classes labeled with the names of the family members and not only them they can train the images of their relatives which provides the access to unlock their door. By using this model one can secure the home premises from the invaders and also capture the suspected people who are not authorized to move inside the house. By using “dlib one short learning”, all the faces for permission would be trained and the model is given to the security system where it can secure the premises with good accuracy through trained images.*

Keywords: *Deep Learning, Computer Vision, Image Recognition.*

I. INTRODUCTION

A general statement of the face recognition problem (in computer vision) can be formulated as follows: given still or video images of a scene, identify or verify one or more persons in the scene using a stored database of faces. Facial recognition generally involves two stages:

'Face Detection' where a photo is searched to find a face, then the image is processed to crop and extract the person's face for easier recognition. 'Face Recognition' where that detected and processed face is compared to a database of known faces, to decide who that person is.

Face detection can be performed fairly easily and reliably with Intel's open source framework called OpenCV and Haar Cascade Classifier which is used to identify objects in an image and video. This framework has an inbuilt Face Detector that works in roughly 90-95% of clear photos of a person looking forward at the camera.

OpenCV has the advantage of being a multi-platform framework; it supports both Windows and Linux, and more recently, Mac OS X. OpenCV has so many capabilities it can seem overwhelming at first. A good understanding of how these methods work is the key to getting good results when using OpenCV.

A. Computer Vision

Computer vision is an interdisciplinary scientific field that deals with how computers can gain high-level understanding from digital images or videos. From the perspective of engineering, it seeks to understand and automate tasks that the human visual system can do. Computer vision tasks include methods for acquiring, processing, analyzing and understanding digital images, and extraction of high-dimensional data from the real world in order to produce numerical or symbolic information, e.g. in the forms of decisions. Understanding in this context means the transformation of visual images (the input of the retina) into descriptions of the world that make sense to thought processes and can elicit appropriate action.

This image understanding can be seen as the disentangling of symbolic information from image data using models constructed with the aid of geometry, physics, statistics, and learning theory.

B. Haar Cascade Classifier

A Haar cascade classifier, is a machine learning object detection program that identifies objects in an image and video. The Smart Security System using Image Recognition OpenCV which consists a type of face detector called a Haar

Cascade classifier. Given an image, which can come from a file or from live video, the face detector examines each image location and classifies it as "Face" or "Not Face."

II. METHODOLOGY

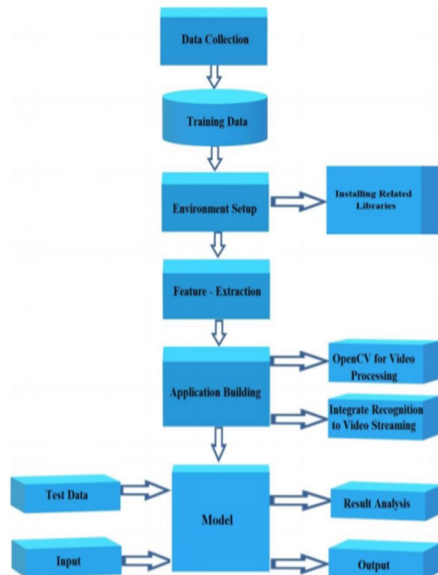


Fig: Methodology

A. Data Collection

The process of gathering data depends on the type of project. The data set can be collected from various sources such as a file, database, sensor and other sources and some free data sets from internet can be used. Dataset can also be collected manually depending on the requirements of the project. In this project, we have manually built dataset. The dataset consists of two folders: Training_images and Test_images. These folders consist of images of the people to whom the access is given and also to whom the access is denied.

B. Train and Test

Data For training a model we initially split the model into 2 sections which are “Training data” and “Testing data”. The classifier is trained using “training dataset”, and then tests the performance of classifier on unseen “test dataset”. Training set: The training set is the material through which the computer learns how to process information. Training data set is used for learning and to fit the parameters of the classifier. Test set: A set of unseen data used only to assess the performance of a fully-specified classifier.

C. Feature Extraction

Determining a subset of the initial features is called feature selection. The selected features are expected to contain the relevant information from the input data, so that the desired task can be performed by using this reduced representation instead of the complete initial data. Properly optimized feature extraction is the key to effective model construction. For image recognition and feature extraction a python code is implemented using haar cascade classifier.

D. Dataset Description

The dataset for this project is built manually. It consists of two folders Test_images and Training_images. The Training_images is classified into two folders “0” and “1”. The folder “0” contains the images of the people to whom we do not give the authorization. And the folder “1” contains the images of the people to whom the authorization is given. Thus the images in the Training_set are to be trained in order to recognize the people in the image and evaluate. The Test_images includes the images of all the people that are trained from the Training_images irrespective of authorization. Thus the Test_images folder goes through all the images and recognizes the person.

III.RESULTS AND DISCUSSION



Fig: Face detection of an authorized person

Description: The above snapshot shows the face detection of an authorized person with status “allowed”.



Fig : Face detection of unauthorized person

Description: The above snapshot shows the face detection of an unauthorized person with status “not_allowed”.



Fig: Face detection of authorized person in streaming video

Description: The above snapshot shows the face detection of an authorized person in a streaming video with status “allowed”.

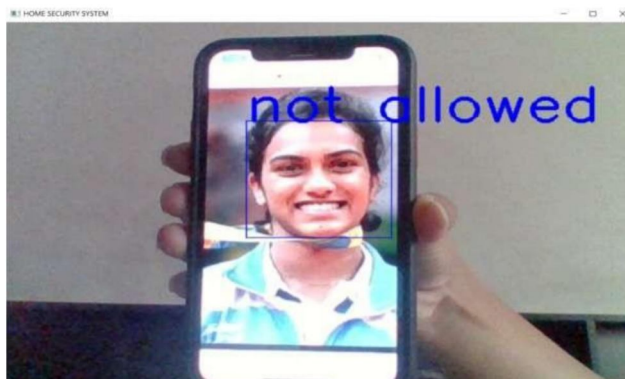


Fig: Face detection of unauthorized person in steaming video

Description: The above snapshot shows the face detection of an unauthorized person in a streaming video with status “not allowed”.



Fig : Alert Notification

Description: The above snapshot shows the alert notification sent to the authorized person when an unauthorized face is detected.

IV. CONCLUSION

In this project, the model is trained with the ability of recognizing face in an image or in a steaming video. The face of a person can be detected in the provided image by using the Face Recognition method which parses through the given dataset and gives the result. Real-time video analysis can be done with the ability to react in real-time by detecting the face of the people in a live video using the trained images. The system senses the intrusion and sends alert notifications to the authorized persons so that action can be taken in response to the intrusion.

BIBLIOGRAPHY

- [1] Smart home automation system for intrusion detection, June 2015, <https://ieeexplore.ieee.org/document/7255156>
- [2] Smart Security and Home Automation System, 2016 <https://ieeexplore.ieee.org/abstract/document/7813916>
- [3] Super Secure Door Lock System For Critical Zones, July 2017, <https://ieeexplore.ieee.org/abstract/document/8076773>
- [4] Design of face detection and recognition system for smart home security application, November 2017 2nd ICITISEE, <https://ieeexplore.ieee.org/abstract/document/828552>



10.22214/IJRASET



45.98



IMPACT FACTOR:
7.129



IMPACT FACTOR:
7.429



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089  (24*7 Support on Whatsapp)