Design and Analysis of IOT Based Real Time System for Door Locking/Unlocking using Face Identification

Ajitesh Kumar, Mona Kumari

Abstract: ***In this era we are facing security issues in every aspect. So for resolving this issue we are proposes a real time application controlled door locking/unlocking mechanism which harnesses the power of IOT and machine learning for smooth functionality. The door unlocking system proposed here uses a Raspberry Pi 3 model B for computation along with a Pi Camera to take face as an input of the user. Also in order to make door unlocking fail proof, fingerprint sensor is used. Scenarios like bad lighting and camera failure can be easily dealt using this sensor. The face detection and recognition system used for door opening will be able to learn user's faces from time to time and update its dataset. So any subtle changes in the face of user like addition of spectacles or removal of beard can be easily dealt with.***

Keywords:-Raspberry Pi 3, Pi Camera, Machine learning, IOT, Fingerprint Sensor, Cascade Classifiers

I. INTRODUCTION

Automation and security have become an important aspect of life. Internet of Things has proved to be the harbinger of automation coupled with security to the naïve users. Live video monitoring has been around for quite a time. Video surveillance has become quite smart and efficient these days. With the power of image extraction and processing, feature identification of live video has become popular. Video input will be streamed and stored using Pi Camera module. After gathering processed image from live video feed a face recognition algorithm is made to run on that image. Using Haar Cascade classifier for face detection, faces present in the processed image are extracted. Then each face is matched from the previously trained model and confidence percentage is calculated. If confidence percentage is more than 80% then a control message is sent to the servo motor via Raspberry Pi. This control message will start servo motor hence the door knob or handle will be rotated.

This door locking/unlocking system mainly uses the facial identification. We are using the latest camera module to capture the image and verified with stored database and if image match then send a message to the admin and if admin send back a security code in the form of OTP then system open the door and if OTP should not match with stored data then system will never allow the user to open the door.

Revised Manuscript Received on January 10, 2020.

Ajitesh Kumar, GLA University, 17Km. Stone, NH-2, Mathura-Delhi Road, Mathura - 281406 (U.P.) India.
E-mail: ajiteshkumar@gla.ac.in
Mona Kumari, GLA University, 17Km. Stone, NH-2, Mathura-Delhi Road, Mathura - 281 406 (U.P.) India.
E-mail: monakumari@gla.ac.in

II. SYSTEM OVERVIEW

The complete proposed system will consists of Raspberry Pi 3 model B, Pi camera module, a fingerprint sensor, a MG995 Tower Pro Servo motor along with the required circuitry for connection.

Functional modules for operation of the system are as follows:

Step1. Storing user data
Step2. Model for training of user face
Step3.Face detection from video input
Step4. Face recognition
Step5. Giving unlocking permission
Step6.Remotely controlling door unlocking

For above said steps the system regularly updating data set of known faces.

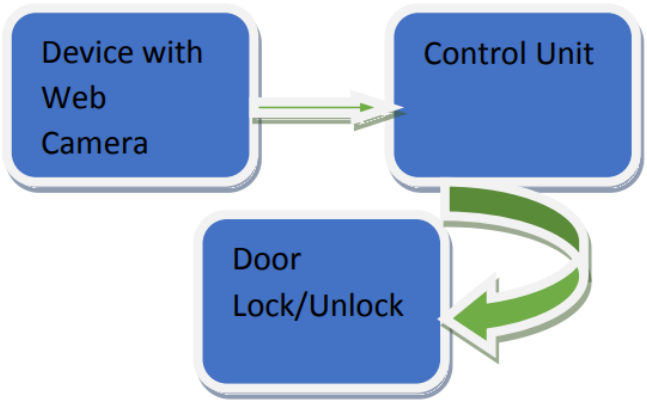


Fig. 1 System Architecture for proposed model

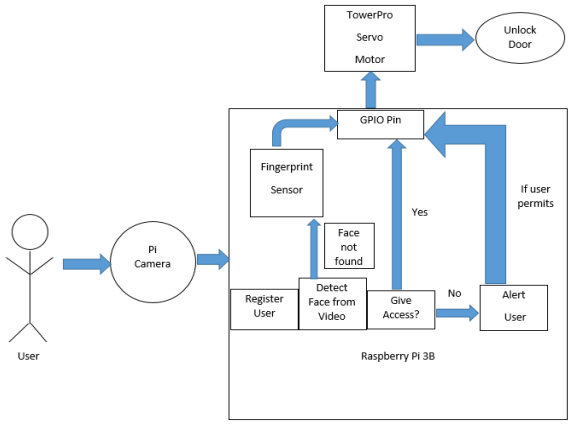


Fig. 2 Blocks Diagram

III. PROPOSED METHODOLOGY

Whenever a person arrives at the door and looks towards the camera then faces of the person is extracted from the feed and stored in the system. Then pre-processing of the extracted face is done. Further the face is matched with existing database of user(s) face. Accordingly access permission is granted to the person in case he/she is a known user. If not then an alert message is sent to the administrator who can remotely give or deny permission for door unlocking. Let's dive into various methodologies for now.

3.1 Storing user data:

We have collected user's facial data from over a thousand images. Also these images have been cropped to a desired size and only relevant details like forehead, chin and eyes have been considered as a sample. All the background details which is not a legitimate face has been dropped for the sampling process.

3.2 Model for training of user face:

In order to make raspberry pi3 learn user's face, LBPH Face Recognizer is used. Local Binary Patterns Histogram is a popular face recognition algorithm which labels the pixels of an image by creating threshold value for neighbouring pixels and result generated is a binary number. For each image of the user (we collected a thousand of them) we are taking 3X3 matrix from top left corner. Considering the middle pixel of matrix as threshold, we classify each pixel value. Converting this new binary value into decimal gives the new pixel value of the middle pixel of the 3X3 matrix. This process of generating matrix is applied to complete image. After that for each image, a histogram is generated from the above generated pixel values. Each histogram represents the features of one particular image.

3.3 Face detection from video input:

In order to capture photo frame of user from a live video we have used a Pi Camera module. After getting a live video input from Pi Camera, haar cascade frontal face classifier is used to get region of interest from the video stream. This face classifier helps in differentiation of faces from non-facial objects.

3.4 Face Recognition:

After the training of LBPH algorithm using genuine faces, now a new unknown image is given as input to the trained model for recognition. This new face is generated from the above step of collection of faces from video stream. A histogram for this new image is generated using the same LBPH algorithm. Now for matching of faces, we compare the histograms of trained faces model and the histogram for new unknown face. Here we are using Euclidean distance formula for comparison.

$$D = \sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$$

This Euclidean distance gives us a confidence value. Lower the confidence value means higher is the possibility of authentic user. It is because here confidence values shows how much closely related the two histograms are.

3.5 Give unlocking permission:

We have set the confidence value to 80% for this system. If the confidence value is more than that, then a trigger message will be sent from general purpose input output (GPIO) pin of raspberry pi to the servo motor. This trigger message will start the servo motor. Ultimately the motor will generate desired amount of torque for rotating the door handle.

3.6 Remotely controlling door unlocking:

If any unknown face is detected then a prompt message will be send to the user of the device. Then user can remotely give unlock permission through the prompt dialog box. This feature will allow remote unlocking of doors for guests or relatives coming in the house.

3.7 Regularly Updating data set of known faces:

In order to handle subsequent changes occurring in the face of the user like growing beard or wearing eye glasses, we will constantly update the data set collected for the user. Here using time as a constraint, we will capture some new faces of the user with time in order to handle changes.

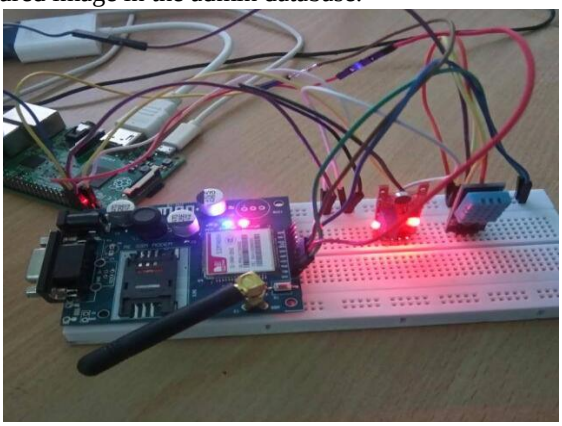
3.8 Handle poor camera vision:

In cases where user is not detected by camera due to bad light we have installed a fail-safe mechanism by the help of fingerprint sensor. In cases where door is not unlocked then user can use the fingerprint sensor to get access through the door.

IV. IMPLEMENTATION AND RESULT

For getting better understanding of proposed model so we need some experimental setup.

Who are authorised by admin firstly stands in front of camera and it will capture the image of person and stored in the admin database images. If the stored images is recognized with captured image the door will be lock/unlocked. When person image not recognized then system send capture image to the admin and wait for the OTP by admin. If admin allow with OTP to the system then system allow the person for lock/unlock and store the captured image in the admin database.



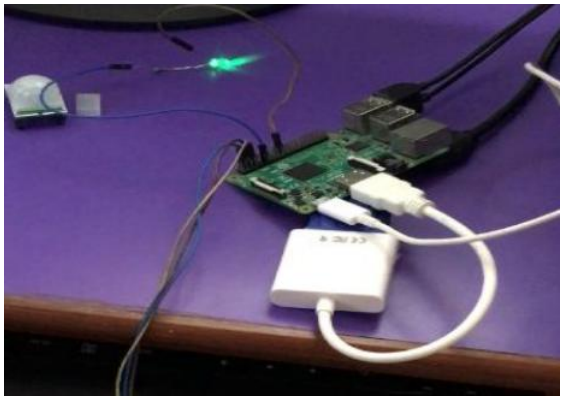


Fig. 3 Working Model

The complete hardware setup is shown above to detect real time faces of persons and send for matching with the databases images. This system tested with different IoT setup.

Table 1: Shows the accuracy of the proposed system

Simulation Setup	Considering Parameters
Images for training	20 images
Images for tested	5 images
Image Size	110*120
Normal condition	85 %
Illumination condition	73%

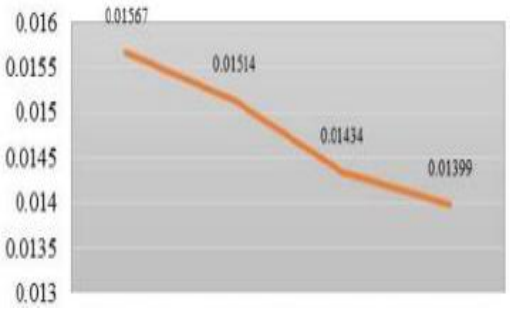


Fig. 4 Time Graph For Praposed Model

This is a time graph of accuracy for performance and time taken for detection of faces as a real data should receive. We get better result as system trained the data which are stored in the database and face detection should be very easy. That simply shows if the image is found in the database system get more accurate and produce result is simple as possible. So that, this proposed model getting more accurate when system trained day by day with real time images.

V. CONCLUSION

Smart door locking/unlocking system will help in developing keyless door locking/unlocking and also remote door unlocking. This IOT based device will remove the need of manually locking/unlocking the door for the registered user. Also for an unknown user, this device will provide an extra layer of security for the residents of the house. An alert message will be immediately send to the registered user when unknown face is detected. This will help in user to decide whether or not to allow a particular person. This device can be installed where restricted access is required without human interference.

REFERENCES

1. A. Boukerche, H. A. B. F. Oliveira, E. F. Nakamura, and A. A. F. Loureiro, "Localization systems for wireless sensor networks," IEEE Wireless Communications, vol. 14, no. 6, pp. 6–12, 2007.
2. L. M. Ni, Y. Liu, Y. C. Lau, and A. P. Patil, "LANDMARC: indoor location sensing using active RFID," in Proceedings of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom '03), pp. 407–415, IEEE, Fort Worth, Tex, USA, March 2003.
3. C.-N. Huang and C.-T. Chan, "ZigBee-based indoor location system by k-nearest neighbor algorithm with weighted RSSI," Procedia *Computer Science, vol. 5, pp. 58–65, 2011.*
4. A. Oka and L. Lampe, "Distributed target tracking using signal strength measurements by a wireless sensor network," IEEE Journal on Selected Areas in Communications, vol. 28, no. 7, pp. 1006–1015, 2010.
5. P. Bahl and V. N. Padmanabhan, "RADAR: an in-building RF based user location and tracking system," in Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '00), vol. 2, pp. 775–784, IEEE, Tel Aviv, Israel, March 2000.
6. Z. Dian and L. M. Ni, "Dynamic clustering for tracking multiple transceiver-free objects," in Proceedings of the IEEE International Conference on Pervasive Computing and Communications (PerCom '09), pp. 1–8, Galveston, Tex, USA, March 2009.
7. C. Xu, B. Firner, R. S. Moore et al., "SCPL: indoor device free multi-subject counting and localization using radio signal strength," in Proceedings of the 12th International Conference on Information Processing in Sensor Networks (IPSN '13), pp. 79–90, Philadelphia, Pa, USA, April 2013.

AUTHORS PROFILE

Ajitesh Kumar, having teaching experience more than 13 years. He has been completed his M.Tech from MNNIT Allahabad in 2012 and pursuing Ph.D from AKTU Lucknow, and having 8 international and 2 national journal publication

Mona Kumari, having teaching experience more than 9 years. She have been completed their M.Tech from MNNIT Allahabad in 2012 with 8.75 CGPI, and having 6 international and 2 national journal publication.