International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 06 | June - 2021 ISSN: 2582-3930

Face Identification based on Fog Computing in Internet of Things

Naga Swathi N
Dept. of ECE
Bapatla Engineering College
Bapatla, A.P., India

Navya B
Dept. of ECE
Bapatla Engineering College
Bapatla, A.P., India

Nidulima D
Dept. of ECE
Bapatla Engineering College
Bapatla, A.P., India

Naga Sai B
Dept. of ECE
Bapatla Engineering College
Bapatla, A.P., India

Rama Kavita B
Dept. of ECE
Bapatla Engineering College
Bapatla, A.P., India

Venkata Ramana Ch
Dept. of ECE
Bapatla Engineering College
Bapatla, A.P., India

ABSTRACT

In the present growing technological world, it is important to own a reliable security system that can protect assets as well as our privacy. The traditional security systems needs an individual to use a key, identification card or password to access an area such as home and workplace. There is chance of loosing the keys or patterns are misused by other persons. In order to minimize the frauds and to improve the security, we are using Fog Computing based face identification for door unlocking system. By using Fog Computing we can increase the processing capacity, storage and communication capability. In this paper, Face detection and recognition algorithm based on LBPH approach is presented. Basically in this technique the image is divided into the multiple pixels and from that pixel threshold value is calculated. By using this value facial expressions like features of eyes, nose and lightning effects are calculated and easily the face is detected. We also used ARDUINO UNO, Servo Motor and ESP8266 module for door opening and closing when the detected face is matched with the images in the database.

Keywords: Face Identification, Face resolution, Fog Computing, Local binary patterns, Internet of Things

I. INTRODUCTION

Now-a-days, because of the recent increase in stealing activities, security is the most critical factor that everyone is looking for. For example, we have various security systems such as CCTV, voice unlock etc., are in use. All of the events that take place in front of it are recorded by CCTV. It does not, however, sound an alarm. If any suspicious activity is detected while using CCTV, anyone can view the recording. Continuous recording, in addition to CCTV, requires a constant high power supply.

Other security technologies, in addition to CCTV, include voice unlock, fingerprint scanners, retina scanners, and RFID systems. These systems have some disadvantages, one of which is high power consumption, which might raise the system's maintenance costs. The proposed method is more efficient than the previous systems and requires less maintenance.

Face resolution is the technique of acquiring precise information about an individual based on the face image of the person being evaluated. Face detection, raw facial picture pre-processing, feature extraction, feature matching, and identity information gathering are all part of this process. The acquired face photos must be compared individually to all of the face templates recorded in the database. The raw facial picture data is in an unstructured format with a higher file size and a more detailed data structure than an ID code. As a result, more computation,

communication, and storage capacity is required. Cloud computing on the other hand is an outstanding services platform the applications can request the services from the cloud. The whole process of resolution takes place under cloud where it requires large network of bandwidth and high processing capability where it cannot be fulfilled by the cloud. So we are using fog computing in between the IOT devices and Cloud in order to increase the storage, processing capability and to save the bandwidth.

The computing power and data storage are closer to the end devices than with cloud computing. The amount of data sent over the network and the time it takes to send it are both significantly reduced. As a result, in this paper, fog computing is used to accomplish face resolution. Face detection, facial image pre-processing, and feature extraction are among the resolution activities that have been transferred to fog nodes. Unlike the standard cloud computing model, which executes all resolution tasks on the cloud and provides raw facial image data, the fog computing model merely sends the feature value to the cloud to match with the face identifiers database. As a result of this process, the network transmission load is drastically reduced. This system is still capable of providing high-quality service, even when bandwidth is limited.

To make the security system more powerful, the suggested system includes additional functions such as alerts and notifications. Algorithms for detection and recognition in combination the term recognition is complicated since it requires an algorithm to extract various attributes from all of the images before selecting the best one. For recognition, a variety of aspects such as the nose, eyes, facial emotions, and viewpoint are used. The majority of the times, these characteristics are the same. As a result, identifying the correct face among all the photos is rather challenging. Apart from that, the recognition approach is more powerful because it can produce accurate results from a large number of inputs. Automatic face recognition is one of the most difficult problems in pattern analysis and computer vision. Another methodology presented in this study is computer vision, which provides face identification and recognition for individuals, which is an exciting application for the Internet of Things. In the proposed system we have used the ARDUINO UNO module, Laptop camera module, Servo motor, ESP8266 module connects this devices to carry the information from one device to another.

II. PROPOSED METHODOLOGY

A facial recognition system is a computer application capable of identifying or verifying a person from a digital image or video frame.

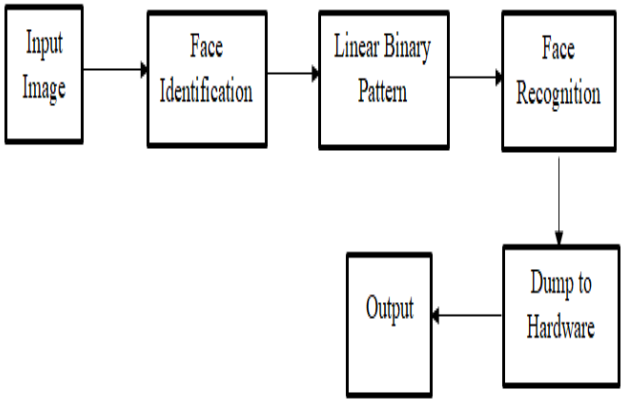

Fig.1. Overview of Face Recognition System

It is typically used in security systems and can be compared to other biometrics such as fingerprint or eye iris recognition systems.Recently, it has also become popular as a commercial identification and marketing tool.

FLOW CHART

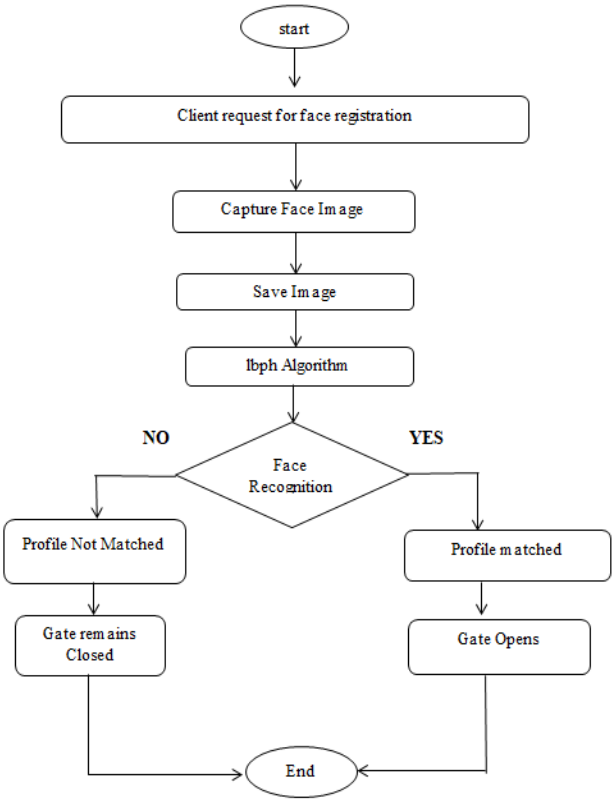

Fig.2. Flow chart of face recognition based door unlocking

This flowchart shows how the face identification and detection is carried out for home security. The operation is started when the request is generated by system to provide the data from the client to store in database. The image of the client or person is extracted by the camera to store/detect the image. For the registration the image extracted is converted into histogram equalization and saved to the database. When the registration is done the data is saved into the cloud server. After the registration the image is compared to all the images stored in the server. The verification of images is carried out by comparing the input facial image with the facial image of client it is one to one comparison. The identification is done by comparing the input image with all the images in dataset to find the user that matches the data/face it is one to many comparison. The comparison is done by using LBPH algorithm. Local binary pattern histogram is a popular algorithm for face recognition and also very easy. An LBPH algorithm consists of four parameters they are radius, neighbours, grid x, grid y.

Radius: It is used to circular binary pattern by representing the radius around pixel. It is basically taken as one neighbour these are the number of sample points to build the circular local binary pattern. If the number of sample points increases the computational cost is also increased.it is usually set to 8.

Grid X: It is formed by number of cells in horizontal direction. Higher the number of cells, Higher the resolution.it provides the feature vector of the image. The grid is usually set to 8.

Grid Y: It is formed by number of cells in vertical direction. Higher the number of cells, higher the resolution.it provides the feature vector of the image. The grid is usually set to 8.

We need to train the algorithm by collecting the images into dataset and providing the unique ID for each image, so that the algorithm recognizes and provides the output. The computation is done but extracting an intermediate image which highlights the features of the face. It is done by using radius and neighbours. The image is converted into grey scale as 3*3pixels, the intensity of each pixel in 3*3matrix is 0-255. The central value of the pixel is taken as threshold. The neighbour pixel threshold value is set to new binary values. If the neighbour is higher or equal then the value is set to 1, if it is lower than the value is set to 0. Now, we obtain matrix containing only binary values. These form the feature vector of the image. The feature vector represents better characteristics of the input image. From these we extract the histogram of the image. The histogram generation is used to compare the input and database images and return the image with closest histogram. The different approaches for comparing histograms are Correlation, Euclidean distance, chi-square, absolute value etc. If the comparison returns matching image then the profile is matched and door gate is opened. If the comparison does not return the matched image then the profile is not verified, the gate remains closed. The same procedure is carried out for all images for identification and authentication.

In this paper, two procedures are implemented as a part of identification of individual face.

1. Procedure for Face Registration

Step 1: Client requests for face registration.

Step 2: The camera captures that user face and save the details.

Step 3: Apply LBPH (Local binary pattern histogram) algorithm to image which is captured and saved.

Step 4: Save that image and details of the user with the user id in a data base.

2. Procedure for Face Authentication

Step 1: Client requests for face authentication.

Step 2: The camera captures that user face and save the details.

Step 3: Apply LBPH (Local binary pattern histogram) algorithm to image which is captured and saved.

Step 4: Save that image and details of the user with the user id in a data base.

Step 5: Compare the input image which stored image in data base with original image.

Step 6: If both the images gets matched then it returns verified successfully and application will work.

To implement the proposed system we used ARDUINO, WIFI Module and Servo motor as the major components. ARDUINO which is used to run the software applications and to show the estimated results through hardware devices which are connected to ARDUINO. In order to transmit data over the internet, WIFI module is used to access microcontroller and Servo motor is used to rotate in two angles with 0 degrees and 90 degrees to show the gate closed or open when the face authentication is done.

III. RESULTS

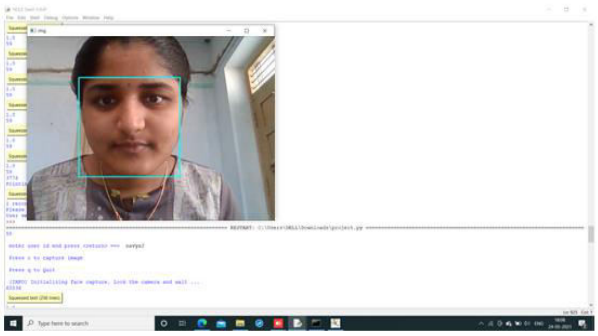

Fig.3. Output screen of input image

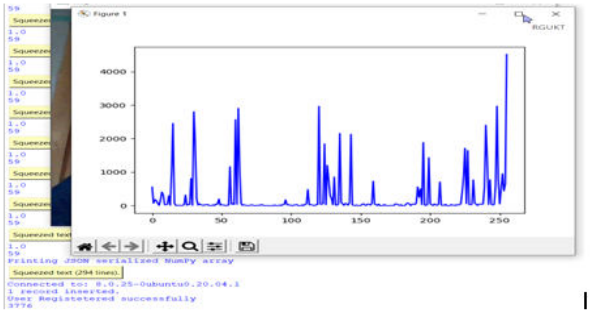

Fig.4. Normalized histogram of user

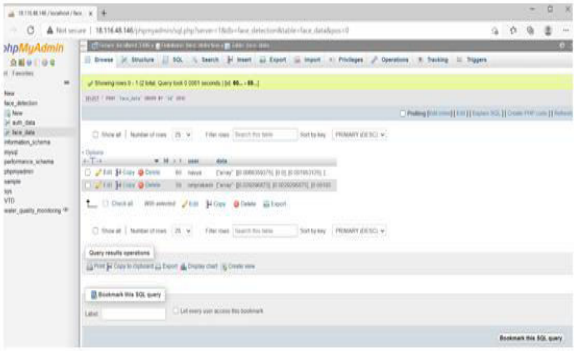

Fig.5. Data Storage Screen

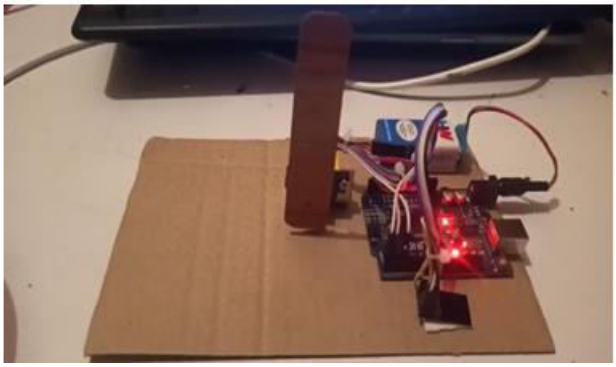

Fig.6. Output screen of gate opened after profile matched

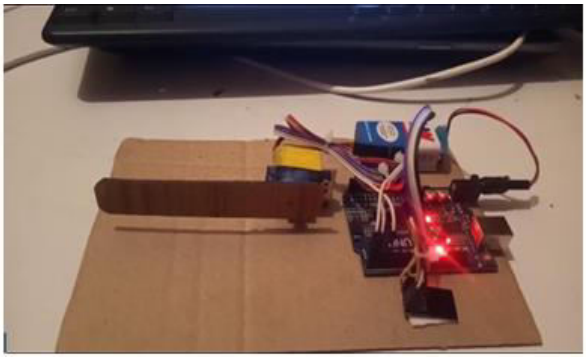

Fig.7. Gate remains closed if profile not matched

IV. CONCLUSION

Fog Computing based face identification for door unlocking system is successfully implemented. Due to the use of face recognition and IOT security will be doubled as compared to the traditional methods. Hence this Fog Computing based Face recognition can be used in places where security is highly needed. It can be used in Smart Surveillance Monitoring Security, Criminal Recognition and Identification System, Attendance System ,Home security alert, Airport security etc..,

V. REFERENCES

[1] Y. Januzaj, A. Luma, Y. Januzaj, V. Ramaj,"Real time access control based on face recognition," in International Conference on Network security & Computer Science(ICNSCS-15),PP.7-12,2015

[2] M. Sahani, C. Nanda, A. K.Sahu, B. Pattnaik.,"Home security system based on face recoginition,""2017 International conference Circuits, Power Comput. Technol.[ICCPCT-2015].,pp.16,2015

[3] Singh, Satish Kumar, and Sanjay Kumar Dhurandher. "Architecture of Fog Computing, Issues and Challenges: A Review." 2020 IEEE 17th India Council International Conference (INDICON) IEEE, 2020.

[4] Zhou, Jun, Zhenfu Cao, Xiaolei Dong, and Athanasios V. Vasilakos. "Security and privacy for cloud-based IoT: Challenges." IEEE Communications Magazine 55, no.1 (2017): 26-33.