Facial Detection and Recognition System on Raspberry pi with Enhanced Security

D. Sri Sai Mahesh
Department of Electronics and communication Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, India.
maheshdantu111@gmail.com

T.Maneesh Reddy
Department of Electronics and communication Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, India.
tammamaneeshreddy@gmail.com

A.Sai Yaswanth
Department of Electronics and communication Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, India.
Saiyaswanth27@gmail.com

Dr. C Joshitha
Department of Electronics and communication Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, India.
joshi1509@kluniversity.in

S. Sudarshan Reddy
Department of Electronics and communication Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, India.
sudarshanreddy.645@gmail.com

2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE) 978-1-7281-4142-8/20/$31.00 ©2020 IEEE 10.1109/ic-ETITE47903.2020.130

***Abstract*— In the present day in our daily life, we all depend on the Internet for web browsing, e-mail, and peer-to-peer services to fulfill our needs. The word Internet means Internetworking of things but IoT (Internet of Things) means a physical object that had a feature of Internet protocol address and that will make the communication between the object and other internet-enabled devices. Here to provide security between the communicating devices without any delay is the main important factor. To provide more security to the existing Face recognition and detection system in homes and banks we propose a new system that will extend the current system. In this paper, we have briefly described the requirement to make such a system and Face recognition Algorithm for Authentication purposes and sending the data using Telegram bot.**

***Keywords*— IoT, Raspberry Pi3, OpenCV Face recognition, Telegram bot.**

I. Introduction (*Heading 1*)

The way we interact with the world around us is changing quickly by technology. The word "Internet of Things" refers to the ability to communicate and share information over the internet. The Internet of Things makes people's lives simpler by communicating computers, sensors and operating them from anywhere. Almost everyone is fitted with smartphones nowadays. Some of the well-known messaging apps that can be used in the IoT system are WhatsApp, Telegram, Text messaging App, Emails, etc. in any Internet application Today, security plays an important role here. If we compromised with security in any Internet application such as in industry, bank or Home it leads to vulnerability and causes threats [1]. So any effective IoT communication system must agree with the Authorization that is only licensed IoT devices and servers may send or receive information and that is a message from one end should be sent other end by using an encryption algorithm.

We consider one of the situations where recognition of face and detecting it is done. In a simple way, facial recognition means identifying and confirming whether a person in a digital image or in a video frame is the same in the Database or not. Face detections are the first and foremost step for face recognition. Previously, people used nonliving things such as plastic cards, tokens, smart cards, Pins and authentication keys to get access grants in a confined area such as DRDO, ISRO, SpaceX, NASA, and in Industries. Eyes, Nose, Forehead, and mouth which leads to facial extraction. In a system with recognition of face and detection is cheaper, simpler, more precise, and non-interrupting process contrast with biometrics. Commonly most members used Open Source Computer Vision Library, in short, it is called OpenCV which is used for execution or operation related to pictures. In other words, we have to install a library called OpenCV to do Image processing. Regularly used facial detection algorithms by OpenCV are Haar Cascade Classifier, LBP Cascade Classifier but here in this work I used Harr Cascade Classifier and face recognition algorithms are Haar-like features, Fisher face, and Eigen's face. Several face recognition techniques provide analyzing the geometric features of facial images, such as location and distance amongst, nose, eyes, and mouth. After this Ojala etal in [2] produced one of the extraction feature methods called a local binary pattern (LBP).

A. *Eigen face:*

In 1901 Karl Pearson invents a principal component analysis which is sometimes called PCA. In [3] and [4] it says eigenfaces mainly it depends on PCA. PCA is a numerical methodology it utilizes an Orthogonal transformation to change over a lot of likely related M face pictures into a set of K uncorrelated elements called Eigenfaces. These Eigenfaces are less than original faces in the dataset i.e. K<M. The use of PCA is it transforms the training set images in the database to lower-dimensional Picture so that it will reduce the calculations which are used for finding Eigenfaces. After transformation of the training set the eigenfaces which are at first few show the more direction of the data and after proceeding those eigenfaces remaining all show the less direction with more noise so we will discard them. The first

978-1-7281-4142-8/$31.00 ©2020 IEEE

few eigenfaces can be able to represent the whole dataset because it had considerable features are the direction in it so, therefore, each face in the dataset can be formed by adding all these eigenfaces. Here we had some disadvantages are there consider if the feature set has data in million then the variance scale will be bluck in training set where eigenfaces show biased towards features that lead the false results. Therefore it is demanding CPU and it demands quite excessive processing power contrast to CMM (computational matrix mathematics) which is used in the Local Binary Pattern Histogram.

B. *Fisher face*

In 1936 Ronald A. Fisher developed liner Discriminant Analysis. In [5] it says Fisher face depends upon LDA where it is used to search projection in a line so there will be a good separation of samples in random classes. It also used in pattern recognition. Random lighting conditions have a minimum effect on the sorting process. LDA also converts the higher dimensional pictures to a lower-dimensional one so, similarly, like above PCA it depends on CPU with higher processing power.

C. *Local Binary Pattern Histogram(LBPH)*

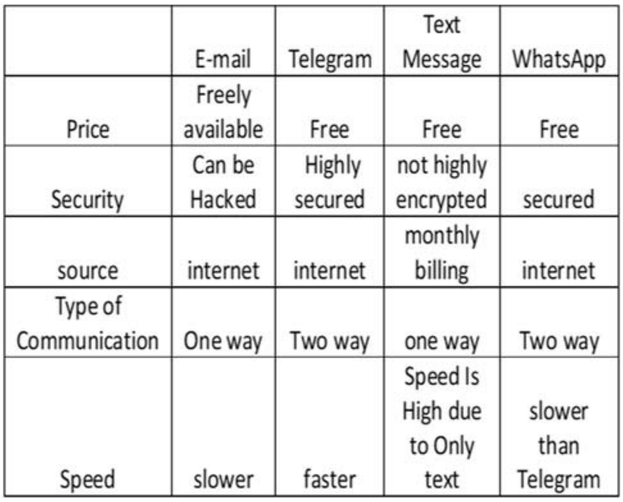
The local binary pattern looks at a little block of 3*3pixels and it is particularly interesting at the central pixel. so let’s say that the pixel value of our central pixel is any value ‘x’ and it has eight pixels around it, and it is a nine-block. Let us put some numbers around ‘x’ like 100, 10, 50, 68, 33, 59, 23, 222 in a clockwise so it makes some sense an LBP is now going to change this set of 3*3 pixels into a one value and it will do it by first comparing every neighboring pixel with the middle pixel that can be either intensity value or luminosity value .so we are going to compare every neighbor of this center pixel with the center, for understanding let us say it is 35 and if it is higher than or same the middle value I .e.35 then we will assign a 1 and if it’s smaller than that it will assign a zero. And we'll transform these 8 bits to form one byte and we can convert any order of these numbers into a number string that will then be converted into a decimal number for the training of our system. The nice thing about these local binary patterns is that it is illumination invariable. It means if you change the brightness on the set all these pixel values will rise but the relative value change among the pixels will endure the same. if there are enough pixels in that block if the block is big enough, we will turn these values into a histogram so looking at the statistics how many times did a number came out of 256 different values. so, we get quite robust statistics in practice we use something called uniform local binary patterns because they only 59 different possible values rather than 256.

The reason why we are using Telegram compare with others is shown in Table 1. And there is no official announcement in creating and maintain Bot in WhatsApp. So Because of this, we preferred Telegram bot from [6].

D. *Telegram*

We use Telegram, it is a chat-based application user can download it, which is available in play store. Inside the telegram, we have Telegram bots which are a mediator application that works innards the Telegram and users can collaborate with Telegram bots by sending them inline requests commands, and messages. MTProto is the protocol used by Telegram Messenger that encrypts conversations with AES-256 (Advanced Encryption standard). One can send HTTP request to bots API so that bot allows smartphones to manage not only by the individuals yet also by the machines like a Raspberry Pi 3.

TABLE 1 Comparation Different Data Transferring Apps



	E-mail	Telegram	Text Message	WhatsApp
Price	Freely available	Free	Free	Free
Security	Can be Hacked	Highly secured	not highly encrypted	secured
source	internet	internet	monthly billing	internet
Type of Communication	One way	Two way	one way	Two way
Speed	slower	faster	Speed Is High due to Only text	slower than Telegram

E. *RASPBERRY PI 3*

In [6] and [7] Raspberry pi hardware is a single board computer that is developed by the Raspberry pi foundation. Raspberry pi 3 has Quad-core 64-bit RAM Cortex A53 processor which is clocked by default at 1.2 GHZ and with GPU of 400 MHZ, Video Core IV multimedia and it has memory of 1GB LPDDR2-900 SDRAM (i.e.900MHz). It has four USB ports it supports the network with 10/100Mbps Ethernet and 802.1 In Wireless LAN. 40-pin GPIO header is on current Raspberry pi. In the proposed model we connect GPIO pin to PIR sensor.

F. *PIR Sensor*

PIR Sensor (Passive infrared sensor) use the pyroelectric sensors of pair to detect heat energy in the surroundings. These two pyroelectric sensors kept beside each other end measure the 3different the signal of the two sensors so that it will engage from [8].

II. DESIGN METHODOLOGY

To understand my work what I had done Consider a situation in a bank or home where security is required to access the door. Figure 1 shows how the different modules are interfaced with the raspberry pi and their data flow connections with each other. In the Proposed system, I used PIR Sensor which will detect the human or animal based on body temperature and it will send a signal to raspberry pi and make the raspberry run the code of face recognition and detection.

The initial step of face representation is how to get the face and check which type of algorithm is required to detect it. so, for that haar-like feature and AdaBoost classifier are enveloped to recognize face detection. There some factors which affect the precision of the face recognition system for e.g. redundant date, shine, image size, etc. so because of this we caught picture before the face recognition and convert this face into grayscale and after we normalized it. After this feature attraction takes place. In this, the face image is compared with the image which is stored and obtained the features.

The feature extraction is the main part of the face recognition system where sampling of the face and calculate the similarities among the images are taken place. LBP is one Block diagram and Data Transfer between the Method of the techniques used in face recognition for expressing the shape and character of digital images. LBP and haar-like features are powerful and efficient when compare with others in real-time applications. In the LBP technique, it will be partitioning the picture into a small number of zones and features are extracted in each region of the image (i.e. it will extract features in each partitioned individual region part) and then after it will characterize the surroundings of the pixels and they coded into binary patterns. They combined all features and form a signal histogram which is used for expression of the picture. In the classification stage and comparison is performed between the face image and the before stored image and the highest identical count is the output of the classification portion. Face recognition is performed after extraction of the LBPH feature vectors and they resort the KKL (K-Nearest Neighbour) classified depending on the histogram matching method. In KKL input faces will be compared with the training data and select the face. After detecting the face if the person is authorized will be able to access the door. if any unknown face is found then the picture of the face is taken and sent to the security guard (if you consider it as the home it is sent to any member of the home). To send the image from raspberry pi to telegram we must follow certain steps, firstly we must install telegram libraries in the raspberry pi to use Telegram. After this all the users who are going to handle the situation (i.e. Security guard) must have a Telegram account there must be login with their mobile numbers. All the security guards should get Telegram Bot API token by typing "@botfather" and bot father will help you in creating a new account or type "/new bot" which will create a new bot choose a name for your bot and then after choosing username then-new bot is created. Then after finding your chat id and keep in python code.

In this project, we had introduced two Method based on the user requirement and application any one of them can be used. Method 1 it says about series alert detection. We design the code in such a way that when person1 did not see the message or if he did not give a proper reply to the message within the given time then the message will be sent to the person 2 after time completed. Like the above case if person 2 did not reply properly then he will ask to reply correctly by Bot. Like the above case within the time if he had not to reply properly then after the completion of time it will send to person 3 similarly like above. if person 3 did not reply within the time then alarm (buzzer) will be on so that everyone comes to know that something is happening in the bank or home. Here every person Telegram chat is saved with the time in the file. The proposed model is effective in security and time saving without any delay and more accurate. If the authorized person is found and detected, then it will be taking the image and stock in the database and you will get the acknowledgment of the welcome message.

Figure 1 Block diagram and Data Transfer between the modules

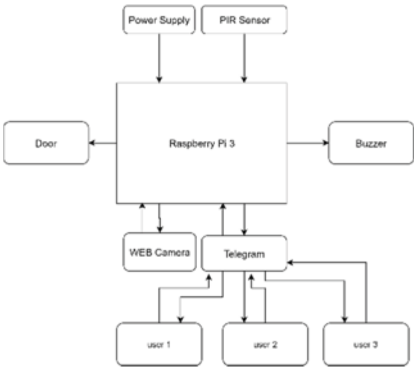


Figure 2 Flow diagram of the working model of series method.

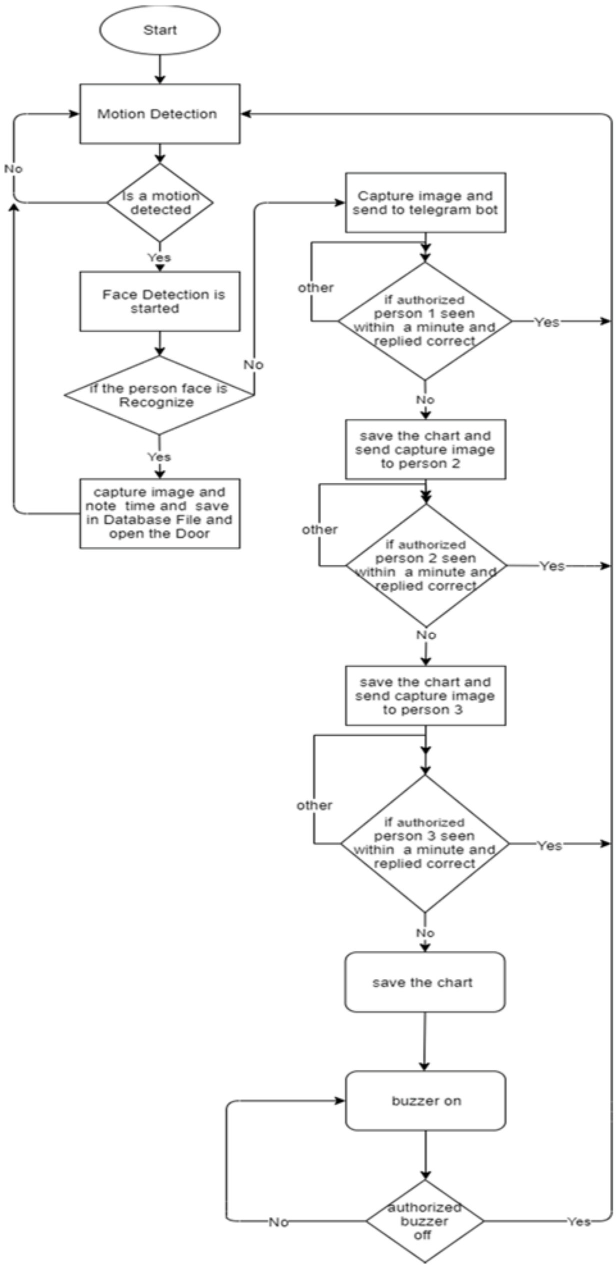
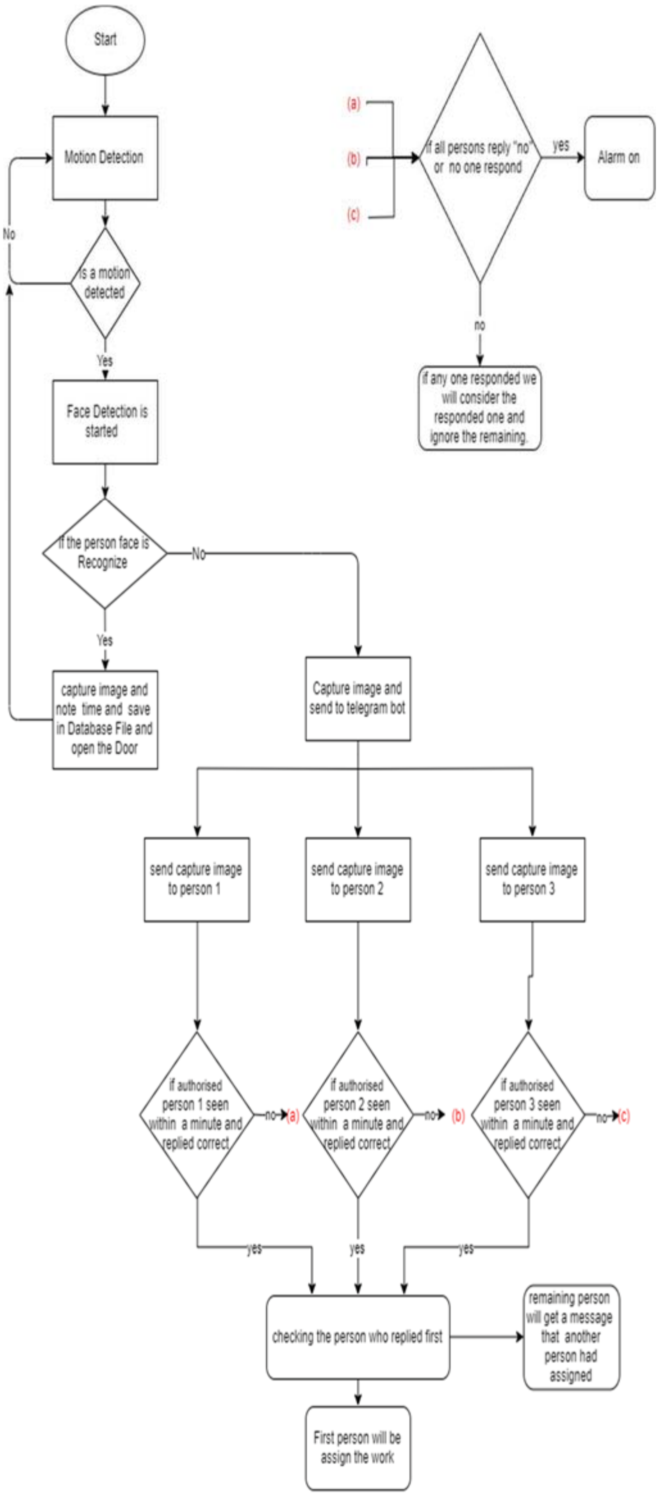

Start
Motion Detection
No
Is a motion detected
Yes
Face Detection is started
No
If the person face is Recognize
Yes
capture image and note time and save in Database File and open the Door
Capture image and send to telegram bot
other
if authorized person 1 seen within a minute and replied correct
Yes
No
save the chart and send capture image to person 2
other
if authorized person 2 seen within a minute and replied correct
Yes
No
save the chart and send capture image to person 3
other
if authorized person 3 seen within a minute and replied correct
Yes
No
save the chart
buzzer on
No
authorized buzzer off
Yes

Figure 3 Flow diagram of the working model parallel model.


Start
Motion Detection
No
Is a motion detected
Yes
Face Detection is started
If the person face is Recognize
No
Yes
capture image and note time and save in Database File and open the Door
Capture image and send to telegram bot
send capture image to person 1
send capture image to person 2
send capture image to person 3
if authorised person 1 seen within a minute and replied correct
no
(a)
if authorised person 2 seen within a minute and replied correct
no
(b)
if authorised person 3 seen within a minute and replied correct
no
(c)
yes
yes
yes
checking the person who replied first
remaining person will get a message that another person had assigned
First person will be assign the work
(a)
(b)
(c)
If all persons reply "no" or no one respond
yes
Alarm on
no
If any one responded we will consider the responded one and ignore the remaining.

The flow diagram in the Figure 2 briefly describe the working of the face recognition system and the enhancement in security as we had discussed in the above.

Method 2 is about parallel alert detection. In this case we initially we send the unknown to all the authorized persons and we are waiting for the response from them by considering the following cases

case1: when all authorized persons responded by typing "yes" then we will consider the one who responded first within a given time, for example, consider the time is 1 Minute. The person who responded lately is ignored by sending this a message that another person had been assigned thank you for the response.

case 2: when all authorized person is not responded within a given time or when all replied "no" ("no" means they are not able to handle the situation due to some work) within the time then the alarm will be rang and message will be sent to everyone that no one had responded.

case 3: when the authorized persons press "no" within the given time we will ignore those persons and consider the persons who will replies "yes" and try to see in consider one who replies first.

In series, model data is sent to the limited persons based on the conditions. Whereas in the parallel model we will send data to all authorized persons because of this if we consider the parallel model we have to compromise with data.

In the serial model, if we consider a minute for each person then the maximum time taken is 3 minutes whereas in parallel model maximum time taken is 1 minute because we are sending parallelly the message so if we consider parallel model we will get the high-speed data.

III. EXPERIMENTAL RESULT

The main aim of this proposed system is to provide more security to the existing system [1]. In the proposed model the results of each part of the flow chart are shown below. When an authorized person enters the door, it will open the door and the results of this are shown in Figure.4 and the output of the acknowledgment is shown in Figure.5.

Figure 4 Authorized person detected image.

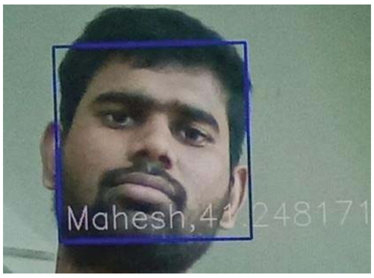
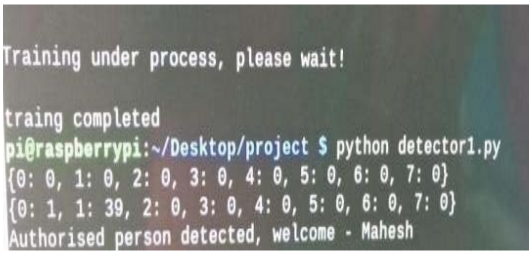


Figure 5 Acknowledgment received by Authorized person.



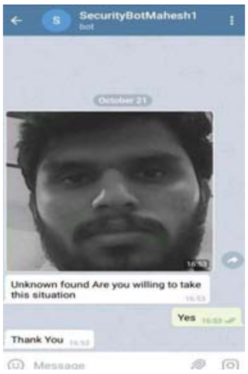
```
Training under process, please wait!

traing completed
pi@raspberrypi:~/Desktop/project $ python detector1.py
{0: 0, 1: 0, 2: 0, 3: 0, 4: 0, 5: 0, 6: 0, 7: 0}
{0: 1, 1: 39, 2: 0, 3: 0, 4: 0, 5: 0, 6: 0, 7: 0}
Authorised person detected, welcome - Mahesh
```

When an unauthorized person tries to access the door then the image of the unauthorized person will be stored in the database folder and this image will be sent to the security officers. The Figure.6,7 and Figure.8 show the possible causes of the response given by the security guard and when he has seen the message.

Case 1:

Figure 6 Unauthorized image and Notification sent by Raspberry pi to security guard Telegram bot.



Unknown found Are you willing to take this situation

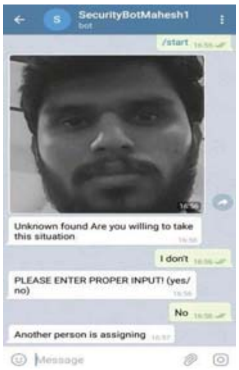
Yes

Thank You

In this case, Bot will ask that an unknown face is Found so whether it going to this situation are not. When the response is delayed within the given time then a message is sent to the Second security guard and the same thing is applied to this person.

Case 2:

Figure 7 Image and Notification sent by bot when proper replay is not given.



/start

Unknown found Are you willing to take this situation

I don't

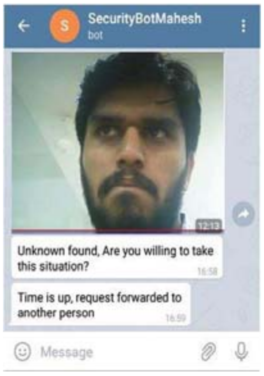
PLEASE ENTER PROPER INPUT! (yes/no)

No

Another person is assigning

Case 3:

Figure 8 person not responded image send to another person



Unknown found, Are you willing to take this situation?

16:58

Time is up, request forwarded to another person

16:59

When the security guard replied other than Yes or No then it will as reply correctly. If suppose a person replied that he is not willing to take this situation then it will send the same message to another security guard. Here see the difference of the different bots on is Security Bot Mahesh1 and another is Security Bot Mahesh when the person did not reply then it will see for a minute and send to another person by saying that time is up so request had been forwarded to another person. If no one is responding, then the Alarm will begin.

IV. CONCLUSION

In summary this paper, we implemented the Face Recognition and Detection system for security by connecting with raspberry and if any Unknown face is detected to make it more secure and easy, we connected with Telegram bot. The main focus of this paper is after receiving the message if a person not responding then transferring the message to another person till all reaches the message is one of the solutions and another solution is a messaging all and waiting for a certain time for response of the first person is the possible solutions provided in this paper.

ACKNOWLEDGMENT

We Acknowledge Government of India FIST – SR/FST/ET-11/2019/450.

REFERENCES

[1] Nashwan Adnan OTHMAN, Ilhan AYDIN "A Face Recognition Method in the Internet of Things for Security Applications in Smart Homes and Cities" in Proc.2018 6th International Istambul Smart Grids and Cities Congress anFair(ICSG).

[2] T. Ojala, M. Pietikainen and D. Harwood, "A comparative study of texture measures with classification based on feature distributions," Pattern Recognition vol. 29, pp. 51-59, January 1996.

[3] Raj G Anvekar, Dr.Rajeshwari M Banakar "Design Alternatives For End User Communication In IOT Based System Model" in Proc. 2017 IEEE International Conference on Technological Innovation in ICT For Agriculture and Rural Development(TIAR 2017).

[4] Monica Chillaron, Larisa Dunai, Guillermo Peris Fajarnes, Ismael Lengua Lengua "Face detection and recognition application for Android" in Proc. IECON2015-Yokohama November 9-12, 2015.

[5] Gagandeep Singh Nagpal, Gagandeep Singh, Jappreet Singh, Nishant Yadav "Facial Detection and Recognition using OpenCV on Raspberry Pi Zero" in Proc. International Conference on Advances in Computing, Communication Control and Networking (ICACCCN2018).

[6] Neha Patil, Shrikant Ambatkar and Sandeep Kakde "IoT Based Smart Surveillance Security System using Raspberry Pi" in Proc. International Conference on Communication and Signal Processing, April 6-8, 2017, India.

[7] Ms. Ashwini Pawar, Prof. V. M. Umale "Internet of Things Based Home Security Using Raspberry Pi." In Proc. 978-15386-5257-2/18/$31.00©2018IEEE.

[8] Paul Viola. Michael Jones "Rapid Object Detection using a Boosted Cascade of Simple Features" in Proc. 0-7695-12720/01 $10.00 0 2001 IEEE.

[9] Vinit Jain, Soniya Chawla "IMPLEMENTATION OF A SMART SAFETY AND SECURITY DEVICE USING RASPBERRY PI, TELEGRAM BOT, PROTA OS AND MANYTHING WEB SERVICE" in Proc. International Journal of Computer Engineering and Applications, Volume XII, Issue II, Feb. 18, www.ijcea.com ISSN 2321-3469 .