Intrusion Detection System using Raspberry Pi and Telegram Integration

Mfundo Zuma
Department of Computer Systems Engineering
Tshwane University of Technology
Pretoria, South Africa
mgzuma@gmail.com

Pius A Owolawi
Department of Computer Systems Engineering
Tshwane University of Technology
Pretoria, South Africa
owolawipa@tut.ac.za

Vusi Malele
Department of Computer Systems Engineering
Tshwane University of Technology
Pretoria, South Africa
vusimalele@gmail.com

Kehinde Odeyemi
Department of Computer Systems Engineering
Tshwane University of Technology
Pretoria, South Africa
kensonics@yahoo.com

Gbolahan Aiyetoro
Department of Computer Systems Engineering
Tshwane University of Technology
Pretoria, South Africa
g.aiyetoro@ieee.org

Joseph S. Ojo
Department of Physics
Federal University of Technology, Akure (FUTA)
Akure, Nigeria
josnno@yahoo.com

Abstract

Security is of enormous importance in this modern age. The crime rate increases exponentially, and traditional home surveillance systems are expensive and limited in intelligent capabilities, such as real-time detection, instant alert, and prompt reporting. As a result of the rapid evolution of cutting technologies and devices, such as Raspberry Pi and several enabled APIs, the limitation, as mentioned, has become a thing of the past. This paper implements an Intrusion Detection System (IDS) using a Raspberry Pi processor that serves as a controller and stations at a home environment. The choice of Raspberry Pi 4 is considered, which is the core of the system; it does all processing between all components (i.e., Passive Infrared sensor, Web camera, Light Emitting Diode) connected to it. The intelligent device is integrated with the Telegram bot via its API. The API with the appropriate Telegram framework is used as an instant messenger generator and notification system. The designed system achieved promising results, as it accurately identified known people, and all unidentified people were flagged by sending a Telegram text message, which included the captured image of the unknown intruder. The overall accuracy rate achieved was 84 per cent, and the accuracy rate for known people was 86 per cent.

icARTi '21, December 9–10, 2021, Virtual Event, Mauritius

ACM ISBN 978-1-4503-8575-6/21/12…$15.00
https://doi.org/10.1145/3487923.3487928

CCS Concepts: • **Architectures**; • **Embedded and cyber-physical systems** ;

Keywords: Raspberry Pi, Telegram, HOG, OpenCV, Facial recognition, IoT

ACM Reference Format:
Mfundo Zuma, Pius A Owolawi, Vusi Malele, Kehinde Odeyemi, Gbolahan Aiyetoro, and Joseph S. Ojo. 2021. Intrusion Detection System using Raspberry Pi and Telegram Integration. In *International Conference on Artificial Intelligence and its Applications (icARTi '21), December 9–10, 2021, Virtual Event, Mauritius.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3487923.3487928

1 Introduction

According to Statistics South Africa, as stated in the 2019/20 edition, South Africa experienced an estimated statistic of 1.2 million housebreaking incidents affecting an estimated 900,000 households [10]. Unfortunately, none of the records confirms the correlation between the affected houses and those with intelligent and good surveillance systems. Surveillance has been an integral part of safety and security. Traditional surveillance has had several limitations which includes but are not limited to a rigid system setup consisting of closed-circuit television (CCTV), which required constant monitoring of live feeds [11]. Identification has changed throughout the years, where traditional Radio-Frequency Identification (RFID) cards, pins and tokens are no longer in use, because they are prone to disablement and tampering [7], and facial recognition has become the epitome of security, alongside biometrics.

In this era of 4^{th} industrial revolution, the physical connection of things via global networks is termed the Internet of Things (IoT). This technology plays a serious role in today's system integration, and home security is no exception. With the introduction of the Internet of Things (IoT), modern surveillance systems allow people to monitor, communicate

and control devices in their homes in real time scenarios. IoT introduces a more flexible, scalable and robust system (integration of computer, sensors, and smartphones etc.) where one can get real time notification of an intrusion taking place, and this becomes an easy framework due to the capability inherent in IoT [7].

The fusion of facial recognition technique and IoT technology would assist to improve home intrusion systems by sending a response in real-time to the owner, or responsible people or agents, as assigned in the user database. Facial recognition depends on the facial detection (FD) ,which is the process in Computer Vision (CV) that involves analysing a picture and identifying an object (in this case a human face). Facial recognition (FR) is a process of identifying a person in a digital image, or live video feed, using the datasets as the means of comparison or identification.

The Raspberry Pi 4 is adopted in this work as the intelligent device with Raspbian Open-sources operating systems. The written program is done using Python, with other python libraries such as Natural Language tool kits, Open CV and Teleport. The Natural Language toll kits execute command send through the Telegram bot, while OpenCV serves as framework to synthesize machine learning based algorithms and computer vision application. OpenCV provides capabilities of image processing through facial detection algorithms such as Haar Cascade Classifier and Histogram of Gradients (HOG). Both these classifiers have face recognition techniques to compliment them. Figure 1. presents the facial recognition process applied by OpenCV.

Figure 1. Block Diagram of the Facial Recognition Process

Against this background, this project proposes an Intrusion Detection System (IDS), which is a form of home security systems (HSS) that utilizes modern technology such as IoT and Telegram instant messenger (IM). The remainder of this paper is arranged as follows: Section 2 provides the literature review to this project. Section 3 presents the methodology adopted in this study to address the problem at hand, while section 4 discusses findings and discussion of the obtained results and, finally, section 5 concludes the current work and, also, recommends future works.

2 Literature Review

It is well known that various home security systems have been proposed to address home and office security problems. The recent development in the 4th industrial revolution has opened new opportunities for cutting edge technologies to be incorporated into design of intrusion detection. In some cases, mobile devices and applications have played some remarkable roles in smart intrusion systems, in terms of tasks and operations [6]. In recent years, intelligent home advanced technologies and the IoT have provide relief to home- owners to have remote access and control to their home through reliable and secure systems. In addition to this, the daily call from home- owners and the national crime rate has pushed several innovations and research in this direction, to alleviate the problems [4].

As an integral part of smart homes, several intelligent based alarm systems and security systems are already on the shelf with advanced sensors and wireless based networks. These systems are designed to detect intruders and inform respective home- owners, who may then act on the provided information or messages. With little or no intelligent features, these systems have limitations to address the ever- dynamic crimes rate in the 21st Century. What is often observed, is that most of these traditional ways of detecting crime are limited to detect dynamic crime environment and, often, most of them provide false alarms.

In the past, home security was mainly considered to be an alarm that simply triggered when intruders broke into the domain where it was set, whereas, in an intelligent based secure home, or office, it may be armed with smart and intelligent controlled security systems [2]. Attempting to advance home security, various studies have been carried out by many authors on the intruder Detection Systems (IDS), as referenced [2–4, 6, 8].

Based on the contribution of Jaafar et al [6], their work focusses on the design of Dynamic Home Automation alert systems with laser interfaces on webpages and which runs on the Window's 10 mobile application with an intelligent controller of Raspberry Pi 2. The proposed system is visually monitored on the web, and only responds to parameters set on the web. The work comprises three indicators, such as laser, light and alarm, and has the capability of sending messages as well via a mobile. devices.

Daramas et al [4] looks at introduction detection as being integral for a home Automation System, which uses three functional components. One of these components is a Sensor manager. This consists of Passive Infrared sensors, which are used to detect the motion. The other component is a communication coordinator. In this case, the authors used Zigbee technology which coordinates communication among the sensors. The second function was the Firebase, which acts as a cloud database and user authentication platform. The firebase allows the data to be stored, and comparison was done against the stored data. The last function was the Android Application, which was used for monitoring and remote notification. Unfortunately, the system introduced by [4], relied on the PIR sensor to be the main trigger of motion as a result of an intrusion. Furthermore, the system by [4] uses a Zigbee, which has limitations of carrying small amounts of data over short distances, even though its power consumption is very low [4]. To solve the identified challenges, this project uses

a visual component to detect and identify the person flagged by the sensor and uses the Raspberry Pi IP communication port to eliminate the limitations of carrying small amounts of data over short distances.

The contribution by Anitha [2] presents home security as a useful integration of the IoT, while considering using an inexpensive security system. The system is designed in a such a way as to inform the home or factory owner by sending a notification and demanding that the necessary action be taken. The system intelligence is a microcontroller base, integrated with a magnetic Reed sensor to acquire data, a buzzer sounding alarm, Wi-Fi module and, lastly, ESP8266 to synchronize to the internet.

The emergence of Computer vision has introduced several libraries and tools that may be adapted to upgrade the intruder detection systems. A Home Security System using Raspberry Pi, Open Computer Vision (OpenCV) & Multipurpose Internet Mail Extensions (MIME) was proposed by [2]. This system consists of Raspberry Pi for processing, a Passive Infrared (PIR) sensor for detecting motion and to trigger the Raspberry Pi to activate a webcam. The webcam initiated the face detection process and, upon detecting a face, an email with the captured image would be sent to the system owner using Simple Mail Transfer Protocol (SMTP) & MIME. The webcam is controlled by OpenCV, which consists of image processing libraries that allow the image capturing and detection to take place. The system by [3] depends heavily on SMTP servers to be permanently available to ensure that the captured image reaches the system owner. Email has become a traditional communication system with time delays in delivery notifications. Instead of SMTP, email and/or short messaging service (SMS), the proposed system uses the advance notification system, known as Instant Messaging (IM), that ensures immediate delivery of messages and/or notifications.

A Face Recognition System, based on Raspberry Pi Platform, is proposed by [3]. The system consists of a RPi microcontroller, OpenCV & NumPy form image processing using the Python programming language, and SQLite for storing data of the desired people. The system was manually activated and allowed for image capturing to take place. The system introduced by [8] lacks a trigger, which will activate the webcam should there be motion detection, and it also lacks a notification service of people who are intruders, or not, as part of the datasets.

The contribution by Abhilash et al [1] centered on design of a home security system that is economically viable, with an energy efficient scheme, and miniaturized as well. In this case, Pi 3 model B is also used as a controller and integrator, and a Passive Infrared Sensor (PIR sensor) and a webcam are connected. The engraved Pi camera is used to capture images, and the OpenCV python library is used to detect and analyze the captured images. The PIR sensor functions as a motion detector, and the computation is done with python libraries. The captured image, as a result of the triggered sensor, would be sent to the configured email account using the IoT, SMTP and MINE technologies.

With the same concept as referenced in [1], the contribution of Suraj Pawar et al [9], considered the IoT technology, web cameral, the raspberry pi, accompanied by sensors such as Passive Infrared and Ultrasonic sensor, to be the components of their intruder detection systems. In this case, the motion detection camera captures images at a given distance and adopts the local binary patter for the real-time face recognition. In case the intruder is not among those listed in the database, the alarm would trigger with an email containing the image of assumed intruder and a sms as well. The activities of the system are monitored by using an Android application or web application, which allows scalability.

Home Security System using IoT was introduced by [1]. The security system uses Arduino Uno microcontroller, and it is interfaced with components, i.e., a magnetic reed sensor, which monitors status, a buzzer to sound the alarm and an ESP8266 Wi-Fi shield to connect and communicate with the Arduino using the internet. This system has advantages, which include low cost, low maintenance and it is easy to set up. The utilization of the Blynk application also comes as an advantage, as it uses IoT capabilities. However, the system also has limitations. It does not have enough processing power for extra components to be included, such as the USB webcam, and it won't be able to support additional software capabilities for Image Processing algorithms. Table 1 below is a comparison between Arduino Uno and Raspberry Pi system board as published by [5].

Table 1. System board comparison between RPi and Arduino uno

	Raspberry Pi	**Arduino Uno**
Operating System	Raspbian OS	No Operating System
Connections	Computer Based Connections (HDMI, USB, GPIO)	Hardware Based Connection (Power Jack, USB, GPIO)
Data Transfer	FTP, USB or SD Card	Flash of the Microcontroller
Program Execution	Multiple programs can run simultaneously	One program can run at a time
Clock Speed	1.4GHz	16MHz
RAM	4GB	2kB
Number of Input/Output Pins	40	20
Input/Output Max Current	50mA	50mA
Power Consumption	700mW	175mW

Learning from the above similar studies, it could be concluded that, in principle, the IDS requires three criteria for it to be successful:

(i) a sensor which triggers when the motion is detected
(ii) a webcam that captures images and allow OpenCV to process and recognize the captured person; and
(iii) a notification system responsible for alerting should an unidentified person be detected and unrecognized.

The next section describes the methodology adopted in designing and operating the Intruder Detector Systems with appropriate software and hardware used in the design procedures.

3 Methodology

This section describes the method used in this paper. Figure 2 represents the system architecture of the proposed project. The RPi is connected to a Power Supply adapter with an output voltage of 5V DC and electrical current of 3 amps., The webcam is connected to the RPi via USB, with one actuator (LED) and one sensor (PIR) connected to the General-Purpose Input/output GPIO pins of the RPi. The RPi is connected to WiFi and allows it to send messages to Telegram App via Telegram API, which is part of the Telebot module used in the python code. The RPi can be accessed via a Secure Shell protocol (SSH), or Remote Desktop Protocol (RDP) for a graphical user interface (GUI). Figure 3 illustrates the complete system flow diagram for the proposed Intrusion Detection System.

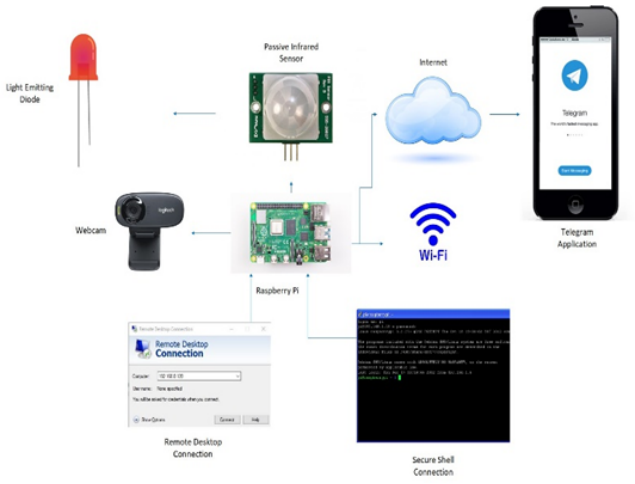

Figure 2. System Architecture

The proposed system will utilise the following components and software.

(a) Raspberry Pi (RPi): The microcontroller is the core of the system; it is the processing unit of the IDS and coordinates all processes [4, 6]. It supports WiFi or an Ethernet connection but, on the current system, it is connected to WiFi. Python programming runs on the RPi, allowing it to control actuators, sensors and Webcam. The RPi communicates with the Telegram application via the Telegram bot API using the Telebot module. After communication processes are completed, the RPi sends a message that includes the picture of the unrecognized person to the Telegram application, as shown in Figure 2.

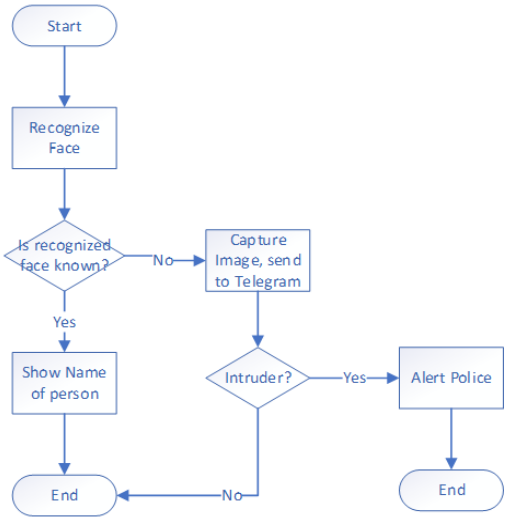

Figure 3. Intrusion Detection System flow diagram

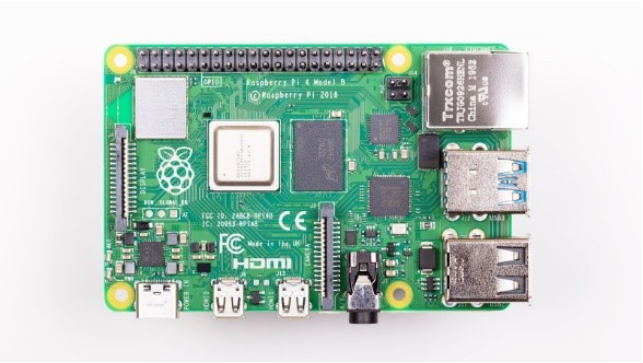

Figure 4. Raspberry Pi 4 Model B

(b) Wi-Fi: The use of Wi-Fi was due to its secure IEEE Standards, flexibility and it also provides high transmission rates. Connection to the Wi-Fi is secure as authentication is required, and the SSID of the home network is hidden from the public domain. This ensures that no intruder can get to the network and control the RPi.
(c) Passive Infrared (PIR) Sensor: This sensor is responsible for detecting motion by measuring infrared light radiating from the object, in this case a human being. The PIR sensor operates at an angle of 100°, with an

operational voltage between 4.5-12V DC. It's a highly sensitive device with low power consumption. In the IDS, the PIR sensor was responsible for flagging any motion detection, this triggered the webcam to activate and capture the person who is considered to be an intruder.

(d) Webcam: The webcam was used to capture images that are processed by OpenCV. This allowed the RPi to use OpenCV library to perform face detection (FD) and face recognition (FR). The webcam was activated once off when motion was detected via the PIR sensor. The webcam was connected to the RPi via USB, and supports 720p HD, meaning the captured images and video were of high quality.

(e) Python Code & OpenCV: The entire IDS was programmed in python with libraries for Image processing, known as OpenCV. During the dataset capture, images were stored in a dataset with the name of the person captured.

Algorithm 1, details how a headshot image is captured and stored in the dataset. In the python code that was created, a dataset name for the person, who will be part of the allowed people as show in line 3 of the algorithm is created. Once the python code runs, the webcam activates and waits for inputs. In this case, the input is the spacebar which captures the image shots as shown in line 4 and 5. The captured headshot images are stored in the dataset folder of the named person as reflected on the last line.

Algorithm 1. Image capturing for image processing and face detection algorithm.
Line 1 Input: Spacebar; Subject_Name
Line 2 Output: Image; Cam_Activation
Line 3 Set **Subject_Name** to "Name"
Line 4 If **Cam_Activation** is launched, Webcam activates & waits for **Input**
Line 5 While **Spacebar** is pressed, capture **Image**
Line 6 Captured **Image** is saved to **Subject_Name** folder

A function called PIRSensor, which contains a block of code that will only run when it is called, is declared. Input pin of the PIR sensor to 'i' is initialized, and an if statement is used to check if the state of the PIR sensor is HIGH or LOW. Should the PIR state be LOW, the LED will be on off state, with a delay of a second. If the PIR state is HIGH, the LED will turn on and launch the video streaming to allow FR to take place.

Another component is used for webcam activation. Encodings, which are used to create mappings between names and faces are initialized to a variable called data. A cascade classifier looks for the facial features of the detected person. The video stream is started on line 126 and the src=0 tells OpenCV to launch using the USB webcam, should it be that an additional webcam is inserted, that second webcam will become src=1.

4 Results and Discussion

The proposed system (see Figure 5) also investigates sending images of unknown people, instead of all detected people. Investigations were also done to ensure detection is done at different angles and distances. Two test cases where conducted, each test case is described and results in Figures 6 and 7 are also discussed. Measurements used for the first test case are as follows, during face recognition:

- False Identity Rate (FIR) is the number of times the system incorrectly identified a person.
- Success Identity Rate (SIR) is the number of times the system correctly identified a person.

Measurements for the second test case involved Pythagoras theorem which is further explained under Test Case Two.

Figure 5. Proposed Intrusion Detection System

4.1 Test Case One

During this test case, the system needed to determine the accuracy of Facial Recognition in our system. This was achieved by presenting five datasets to be tested. It consisted of three known people who are already part of the dataset stored on the Raspberry Pi, and two unknown people.

During the testing phase, the total number of tests conducted per person was five, in total the tests done were 25. Out of the five tests conducted per person, FIR and SIR were identified, and based on the results, there was a high success rate in all cases as compared to false identification. There was a 100 per cent success rate during the facial recognition of the first unknown person (Subject_4), and there was a 60 per cent success rate during the second unknown person (Subject_5). From the three known people (Subject_1, Subject_2 and Subject_3), there was a 100 per cent success rate on facial recognition for Subject_1, and 80 per cent success

rate on both Subject_2 and Subject_3, noting that the FIR detected on Subject_3 is based on the system misidentifying his mother, and flagging the recognition process as someone else.

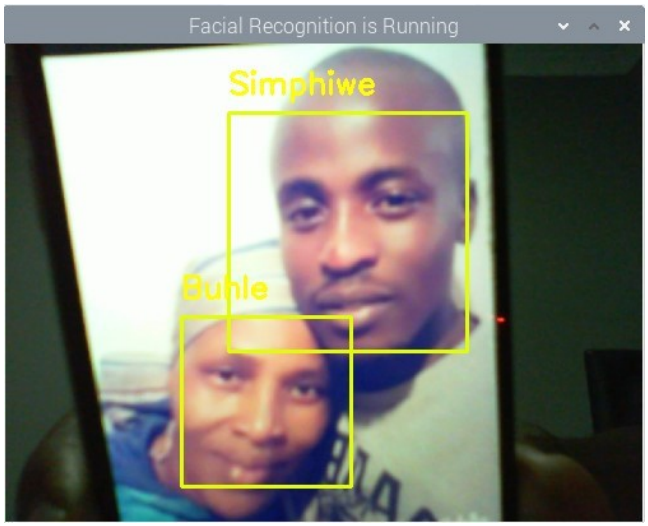

Figure 6. Test case result of known person (Subject_3), and a mismatch on unknown woman

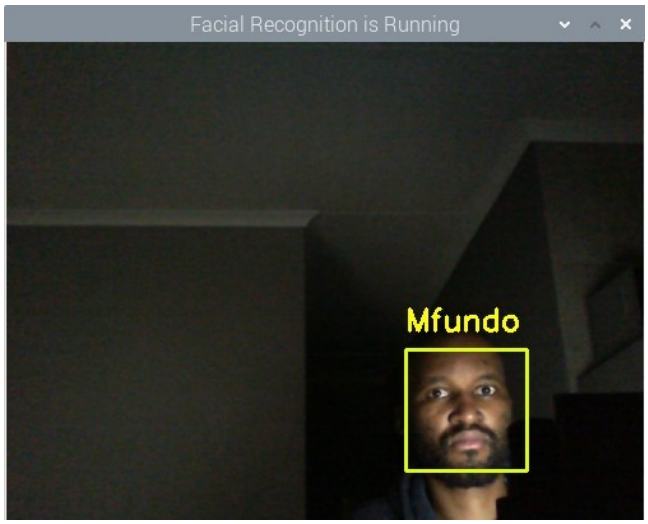

Figure 7. Result of known person (Subject_1) with 100 per cent success rate

4.2 Test Case Two

To test the efficiency and accuracy in the distance range of the FR process, numerous experimental tests were conducted to determine if the FR can recognize a person from different distance ranges (i.e., 0,5m; 1m; 1,5m; 2m and 5m). The test also included different angles for FR, to determine the accuracy of the detection when the face of a person is at a different angle (i.e., 0°, 20°, 45°, 60°, 90°). These angles were estimated using trigonometry ratios. Formula 1 was used to calculate the length of the perpendicular side (AB) as the angle($\angle C$) and base side (BC) have been assumed. Pythagoras Theorem was used as a referencing.

$$tan\theta = \frac{opposite}{adjacent} \quad (1)$$

Table 2. Data used to determine angles at which facial recognition testing can be done

	Length of BC				
Angle ($\angle C$)	0.5m	0.8m	1m	1.5m	2m
0°	N/A	N/A	N/A	N/A	N/A
20°	BA=0.2m	BA=0.3m	BA=0.4m	BA=0.6m	BA=0.7m
45°	BA=0.5m	BA=0.8m	BA=1m	BA=1.5m	BA=2m
60°	BA=0.9m	BA=1.4m	BA=1.7m	BA=2.6m	BA=3.5m
90°	N/A	N/A	N/A	N/A	N/A

The length of 'BA' is not applicable for 0°, due to it not being required in this test case as we were already facing the webcam directly. 'B' represents the Webcam in our test case, and 'C' represents the test subject. The same can be said with regards to 90°. In our calculation, this is undefined and through estimation we can pinpoint 90° at 'C'. But for 90° angle, the facial recognition program is unable to recognise the face when it is turned; this can be caused by the fact that no datasets were included initially at this angle, and it is impossible for the program to analyse the face at this angle. What was also excluded in this case is the cascade classifier, which can detect the features of the face at different angles or detect a facial feature. In our case we only utilized the frontal feature of the cascade classifier.

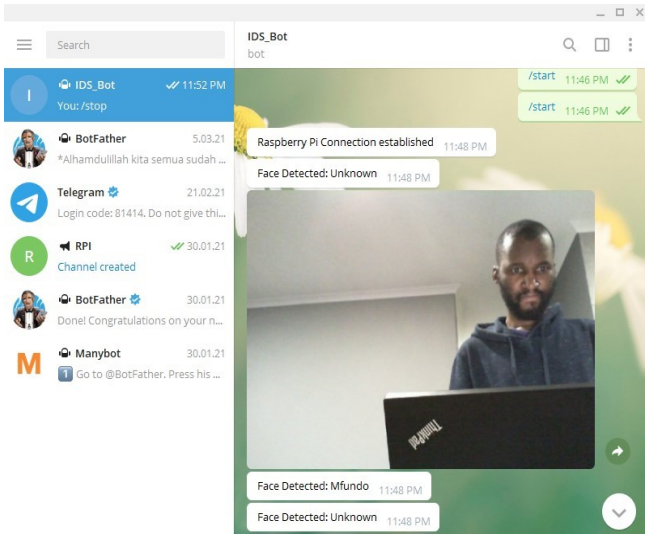

Figure 8. Telegram message and image of false identification

The overall proposed system was activated using the Telegram app, and from there the PIR sensor was either flagged zero for no motion detection, or it flagged one for motion detection. When the motion was detected, the facial recognition process initiated and upon recognising the face, a Telegram message was sent stating that the face was recognised. If the face was not recognised, then a message was also sent stating that the person is unknownand an image is sent along with the message. During testing, the system also sent an image of known people, flagging them as unknown. Figure 8 demonstrates the Telegram message received when facial recognition is unable to identify a person.

5 Conclusion

The study presented an intrusion detection system that has facial recognition capabilities. The study achieved promising results, such as overall face detection being at 84 per cent, and face detection of known people being at 86 per cent. The system was able to achieve its goal of producing an Intrusion detection system based on motion sensor and utilizing instant messaging services such as Telegram to notify the system owner. In future, further investigations need to be done to resolve the misidentification of unknown people, as this will increase the overall facial recognition accuracy from the 84 per cent achieved in this study. Furthermore, cloud database integration will be required to store datasets on the cloud to avoid losing the data should defects arise in the system, and further investigation is required on how the system can autonomously alert security services or police should it be that there is an intruder.

References

[1] D Abhilash, Chandrashekar Chandrashekar, and S Shalini. 2017. Economical, energy efficient and portable home security system based on Raspberry Pi 3 using the concepts of OpenCV and MIME. In *2017 International Conference on Circuits, Controls, and Communications (CCUBE)*. IEEE, 60–64.

[2] A Anitha. 2017. Home security system using internet of things. In *IOP conference series: materials science and engineering*, Vol. 263. IOP Publishing, 042026.

[3] Brian Ray. 2015. The ZigBee Vs WiFi Battle For M2M Communication. https://www.link-labs.com/blog/zigbee-vs-wifi-802-11ah

[4] A Daramas, S Pattarakitsophon, K Eiumtrakul, T Tantidham, and N Tamkittikhun. 2016. HIVE: home automation system for intrusion detection. In *2016 Fifth ICT International Student Project Conference (ICT-ISPC)*. IEEE, 101–104.

[5] David. 2021. Raspberry Pi vs Arduino Comparison. https://diyi0t.com/raspberry-pi-vs-arduino-comparison/

[6] Azfarina Jaafar, Murizah Kassim, Cik Ku Haroswati, and Che Ku Yahya. 2016. Dynamic home automation security (DyHAS) alert system with laser interfaces on webpages and windows mobile using rasberry PI. In *2016 7th IEEE Control and System Graduate Research Colloquium (ICSGRC)*. IEEE, 153–158.

[7] D Sri Sai Mahesh, T Maneesh Reddy, A Sai Yaswanth, C Joshitha, and S Sudarshan Reddy. 2020. Facial detection and recognition system on Raspberry Pi with enhanced security. In *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*. IEEE, 1–5.

[8] Nafis Mustakim, Noushad Hossain, Mohammad Mustafizur Rahman, Nadimul Islam, Zayed Hossain Sayem, and Md Asaduz Zaman Mamun. 2019. Face Recognition System Based on Raspberry Pi Platform. In *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*. IEEE, 1–4.

[9] Suraj Pawar, Vipul Kithani, Sagar Ahuja, and Sunita Sahu. 2018. Smart home security using IoT and face recognition. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*. IEEE, 1–6.

[10] Statistics South Africa. 2021. Housebreaking still number one crime in SA. http://www.statssa.gov.za/?p=13811 [Accessed 28 August 2021].

[11] Xin Zhang, Won-Jae Yi, and Jafar Saniie. 2019. Home surveillance system using computer vision and convolutional neural network. In *2019 IEEE International Conference on Electro Information Technology (EIT)*. IEEE, 266–270.