PRIVATE SECURITY SURVEILLANCE SYSTEM

BENJAMIN KOMMEY*[1], SETH KOTEY[1], ERIC TUTU[1], DANIEL OPOKU[1]

[1] *"Kwame Nkrumah" University of Science and Technology, Faculty of Electrical and Computer Engineering, College of Engineering, KNUST, Kumasi, 00233, Ghana*

Abstract: Security is an essential need for man. Without the sense of security, daily human activities will be greatly affected. Most people go to great lengths to ensure there is a presence of security in their environment, often employing dedicated personnel to keep watch over them and their property. This paper proposes a design of a microcontroller based electronic security system which helps to detect possible intruders to a home. This security system is designed to reduce the need of having personnel stationed as security guards over a home. It has the primary unit called the Area Watch Unit (AWU) consisting of a motion detection unit that effectively detects motion around specified perimeters which is then followed by a computer vision to identify and classify what caused the motion. A facial recognition algorithm is run on the face extracted from the image captured after the object that caused the motion is identified and classified as human. Access is then granted to the individual if the results from the facial recognition is positive otherwise a message is sent to the owner of the home indicating a possible intruder is present. There is also a Final Recovery Unit (FRU) which sends a message to the owner of the home and sounds an alarm whiles flashing lights in the event that the Area Watch Unit (AWU) is by-passed without authority.

Keywords: home security, facial recognition, surveillance, motion detection, computer vision

1. INTRODUCTION

According to Abraham Maslow [1], without a sense of security and safety, individuals will be unable to go about their daily activities- which includes work and other social activities effectively. As a result, the efficient use of the various mechanisms and methods to provide security or protection in our homes is a key aspect of our lives that individuals and communities show massive interest in. Failure to provide a sense of security could lead to unfavorable consequences especially in the socio-economic aspects of our lives. There have been great advances in technology within the 21st century. Current technological trends have made it easier to implement certain difficult tasks and have made people's lives easier [2]. Technology is also one key area in which people are using to improve security [3]. A surveillance system in the home helps to monitor conditions at home, even when occupants may not be present in the home [4, 5]. The use of technology to secure the home removes the need to have personnel stationed for security at home [6]. It also eliminates the delays associated with the reactive approach in responding to home intrusion, whereby witness reports or lengthy closed-circuit television (CCTV) footage is scoured through to identify intruders [7].

*Corresponding author, email: bkommey.coe@knust.edu.gh

Balla and Jadhao [8] developed an IoT based facial recognition security system employing the Raspberry Pi model as the central part of the system to control and coordinates all the activities of the system. A camera is also used to capture an image of the person if he or she presses the doorbell for the facial recognition software to identify the person using facial recognition. The feedback from the recognition process will be sent to the owner via android or web notification who then replies by granting or denying access.

Hussein and Mansoori [9] also proposed smart door system for home security using Raspberry pi3 as the control module which operates over the internet via email modes. The system also has an input phase requiring a newcomer to enter a password or alternatively the system captures an image of the newcomer and matches it with images in the database to either grant of deny access. The system also includes an alarming and message system to alert the owner.

P. Ashwini and V. M. Umale [10] implemented an internet of things-based Home Security using Raspberry Pi. The system consists of peripheral devices like PIR, vibration, fire and gas leakage sensors for detection motion, fire or smoke. The raspberry pi being the processing unit of the system has a pi camera attached to it to capture images and send live video to the owner as and when motion is detected. The buzzer and the lights are also turned on and a message is sent to the user's mail. The system is flawed in the sense that it consists of too many peripherals and components making it bulky and expensive to build. This also make the process lengthy and complicated. Again, the system fails to identify intruder before notifying the user.

S. Sarkar et al [11] designed an android based Home Security System using Internet of Things and firebase. The system consists of a passive infrared sensor and a flame sensor to detect motion and fire so as to secure the home. The NodeMCU incorporated into the system together with firebase send a message to the user in case an intruder is detected through the android mobile application developed using WIFI services. The system is limited in the sense that as a security system, there is no alert system like a light or buzzer in place to duly notify the owner and other individuals around. The use of the WIFI may render the system useless in the event that there is no consistent WIFI connection since the system relies heavily on network.

P. Bhatia, et al [12] implemented an IoT based facial recognition system for home security using LBPH algorithm for face recognition. The raspberry pi microcontroller was used and a camera connected to it is installed near the door to capture images for facial recognition upon which the door is opened if the person matches an image in the database, otherwise an email containing the person's image is sent to the owner for further action. The owner will then decide to open the door or keep it closed. One major limitation of the system is the use of the LBPH algorithm which produces long histograms which slow down long recognition speed especially on large databases. Also, there is no alert system in place to notify onlookers or neighbours.

A. E. Kashef and N. Barakat [13] designed an intelligent alarm system to protect small and valuable items. The proposed system was designed to have a good coverage with two sensors at the front part which are the infrared sensor and the ultrasonic sensors for intrusion detection with an Arduino coordinating the activities of the system. Two sets of sensor data are collected representing the normal and threat situations respectively. Machine learning algorithms are used to analyse and evaluate the data collected. A buzzer is sounded and an email is sent to the user if a high threat situation is detected. The major flaw of the system is that persons regarded as intruders are not identified by any means. Also, the efficiency of the system is dependent entirely on the results from the data evaluation which makes the system ineffective if changes in the environment are not recorded.

Suresh et al [14] implemented a similar system using passive infrared (PIR) sensor, temperature and humidity sensors to detect motion caused by intruders instead of only relying on the PIR sensors to detect motion changes. Text messages are used as a means of communicating with the owner of the home to inform them about the presence of an intruder using the GSM module with all the system's activities been controlled by a single microcontroller.

In this paper, we propose a Private Security Surveillance System (PSSS) to automate security in the home. The system is able to detect the presence of possible intruders into the home. The PSSS is made up of an Area Watch Unit (AWU) and a Final Recovery Unit (FRU). The AWU has motion sensors connected to it to detect objects and cameras to identify people within the perimeter of the home. If a human is identified and not recognised, an alarm is raised and a message is sent to the home owner via SMS or through a mobile application installed on the owner's phone. The FRU is the second line of defence in the event that an intruder bypasses the AWU or destroys it. The FRU raises an alarm, flashes some lights and sends a message to the home owner.

3. EXPERIMENTAL SETUP

The proposed Private Security Surveillance System (PSSS) comprises of an Area Watch Unit (AWU) which is the first point of action in case movement is detected and a Final Recovery Unit (FRU) which is the point of action in the event that the AWU is breached. There is also a face detection and recognition component based on the Principal Component Analysis (PCA) used to identify and recognize faces. The face detection, and recognition is done based on the eigenfaces [15] concept where faces in the dataset are computed and represented as linear faces of eigenfaces after which the nearest neighbor algorithm is performed on the coefficients for recognition. The algorithm handles the detection of the faces of intruders and forwards the appropriate response to the owner's phone. Figure 1 shows an overview of how the PSSS system is installed in the house.

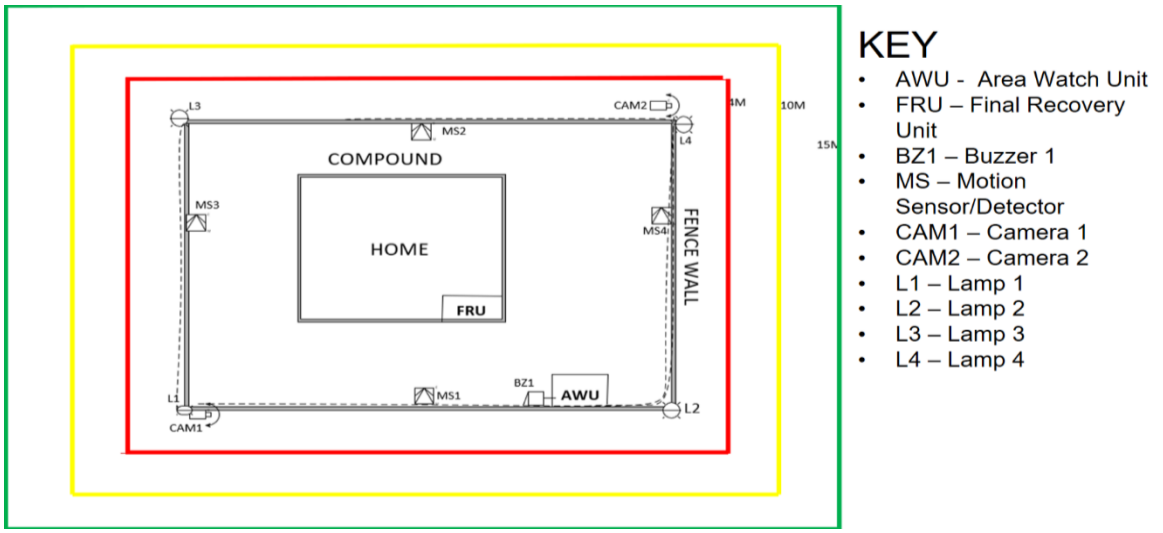

Fig. 1. Private Security Surveillance System (PSSS).

There are lamps (set of led cells) installed at each corner of the perimeter to provide good lighting conditions for the cameras. Four motion detectors are also included in the setup to detect motion of any object.

Block diagrams of the PSSS system are shown in Figure 2 and Figure 3 below. The motion detection unit uses a motion sensor to detect the presence of an object within the outer perimeter (red zone). Once the object is detected, it is identified and classified as human or not. If a human is identified, the AWU then attempts to recognise the human using a face recognition algorithm. The alert (buzzer alert) and message delivery units alert the owner about the presence of a possible intruder. The alert goes off and a message is sent to the owner's mobile phone.

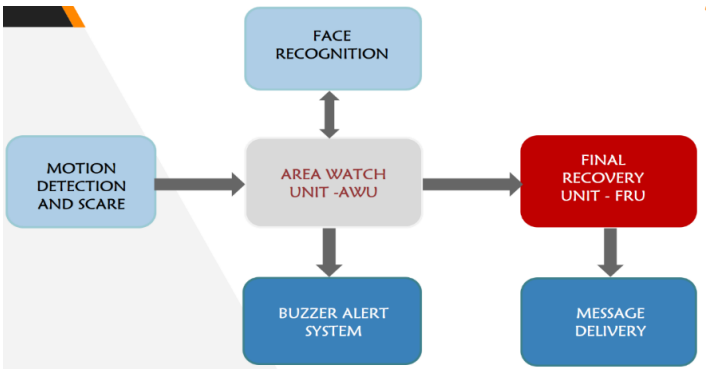

Fig. 2. Block Diagram of PSSS.

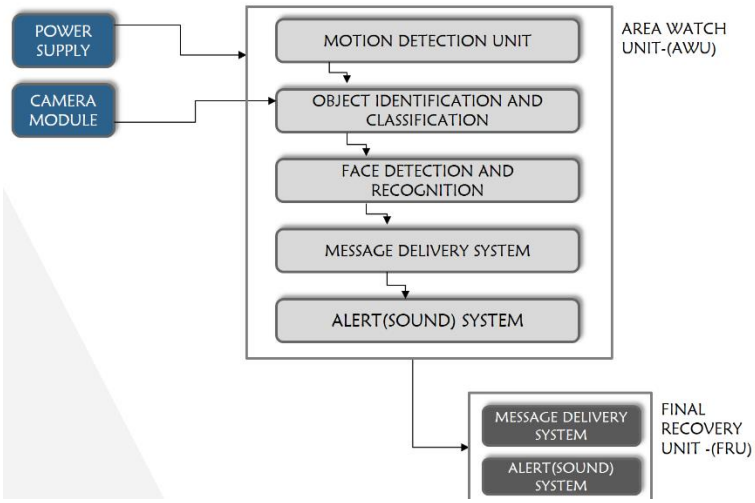

Fig. 3. Expanded Block Diagram of PSSS.

In the event that the Area Watch Unit (AWU) is breached or damaged by an intruder, the Final Recovery Unit (FRU) is brought into action. The Final Recovery Unit (FRU) is mainly made up of two units; the message delivery unit and the alert system. The message delivery unit within the Final Recovery Unit (FRU) is programmed to send a message to the owner or a predefined number in the event that the AWU is breached and an intruder is identified. The alert unit within the Final Recovery Unit (FRU) is made of a buzzer and lights that toggle to draw the attention of occupants in the home to the presence of an intruder.

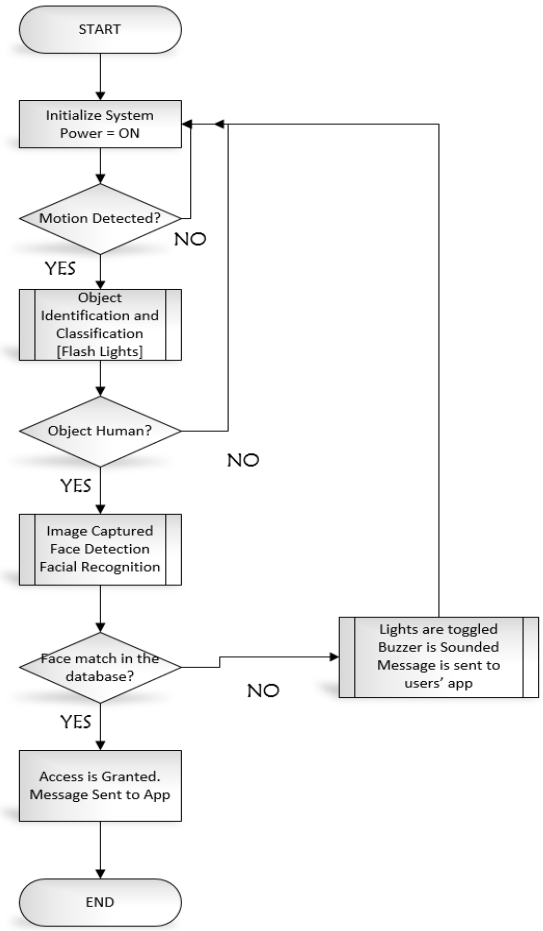

Fig. 4. Flowchart of PSSS.

A flow chart of the processes the system goes through are shown in Figure 4. After the system is turned on, it is initialized. After initialization, the motion detectors are put into action to detect motion of objects. If motion of an objected is detected, an LED cell is flashed to indicate presence of an object. The object is then identified and classified as either human or otherwise. If a human is identified, the face recognition algorithm is applied to the images captured by the camera to determine if the face matches a face in the database. If there is a match, a message is sent to the owner's phone indicating a familiar person is present. If there is no match, multiple LEDs flash and an alarm is sounded to indicate the presence of a possible intruder. A message is also sent to the owner's phone.

2.1. PIR Sensor Operation

Passive Infra-Red (PIR) sensors are low-power, low-cost sensors [16] able to sense motion and are mostly used to detect whether a human has moved in or out of the sensors range [17]. PIRs are basically made up of pyroelectric sensor which detect levels of infrared radiation emitted from humans. The sensor in a motion detector is divided in two halves. The two halves are wired up so that they cancel each other out. If one half sees more or less IR radiation than the other, the output will swing high or low indicating the presence of a human being. There are a number of supporting circuit elements like resistors and capacitors that augment the workings of the pyroelectric sensor. When the sensor is idle, both halves detect the same amount of infrared radiation, already existing the ambient amount radiated in the environment. When a warm body like a human is within range, it first intercepts one half of the PIR sensor, which causes a positive differential change between the two halves. When the human leaves the sensing area, the reverse happens, whereby the sensor generates a negative differential change. These change pulses and temperature are what is detected and interpreted as motion.

The object temperature calculations are made based on the Stefan-Boltzman law:

$$T = \sqrt[4]{T_c^4 + \frac{\Phi}{A\sigma\varepsilon\varepsilon_s}} \tag{1}$$

where T_c is sensor's surface temperature, T - object's temperature in Kelvin, ϕ - magnitude of net thermal radiation flux (net radiated power), ε - emissivity of the object, A - radiating area, σ - Stefan's constant [18].

The output of the PIR sensor is a digital pulse high 3V when triggered as a result of motion detection, thus a recommended power supply of 3.3-5 V input voltage is required. Sensors are fixed to have a 180 degrees of detection range. A LED is used as an indicator of motion detection with: $\mathbf{T_x}$ (Timeout): how long the LED is lit after motion is detected and $\mathbf{T_i}$ (time for LED to stay off when there's no movement).

$\mathbf{T_x}$ and $\mathbf{T_i}$ can be calculated as follows:

$$\boldsymbol{T_x} = 24576 \times R_{10} \times C_6 \tag{2}$$

and

$$\boldsymbol{T_i} = 24 \times R_9 \times C_7 \tag{3}$$

where R_{10}, C_6, R_9 and C_7 are components in the PIR circuitry [19].

2.2. PSSS Facial Recognition

The Principal Component Analysis PCA [20] algorithm is one of the most robust and efficient algorithms used in facial recognition applications [21]. The PCA works by removing the correlations among the different input dimensions thus significantly reducing the data dimensions. Every face image in the dataset with size m*n can be expressed as a vector

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \tag{4}$$

The covariance matrix C_X can be computed as:

$$C_x = \frac{1}{n-1} XX^T \tag{5}$$

where C_X is an m*m matrix which contains all the correlations of an image.

The Eigen faces are then calculated using the covariance matrix and the normalized image matrix.
$\mathbf{C = AA^T}$ is used to obtain the Eigen faces [22, 23].

Normalization of face images is done to transform the two-dimensional face image with size **M*N** to a one-dimensional vector **T**. This is represented mathematically as $\mathbf{A = T_i - m}$ where **A** is the normalized image matrix. Classification of the images is done by using the Euclidean distance measure (L_2 metrics) [24].

$$d(\boldsymbol{X},\boldsymbol{Y}) = L_{p=2}(\boldsymbol{X},\boldsymbol{Y})$$

$$L_{p=2}(X,Y) = \| X\text{-}Y \|$$

$$\| \boldsymbol{X} - \boldsymbol{Y} \| = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \tag{6}$$

where **X, Y** are Eigen feature vectors of length n.

2.3. PSSS Message Alerts

A mobile application is proposed for the system. The PSSS mobile application is to be installed on the owner's mobile phone as a means of receiving alerts from the system. Alerts are sent through the mobile software app and also as an SMS to a number stored in the PSSS.

Figure 5 shows the use case diagram for the mobile software application. This shows the user's interaction with the application. A completely new user to the app will have to sign up first by creating an account before one can use the Private Security Surveillance System (PSSS). After signing up and finishing the other required authentication processes, the user will be taken to the chat screen where the user will be receiving messages from the hardware system. In the case that the user already has an account, one would have to just log in with the details of the account. After the various authentications processes, the user will have full access to all the features of the application. The user can receive messages from the hardware system, view a history of messages received in the past. The information concerning the user can be viewed at the profile section form the drawer menu.

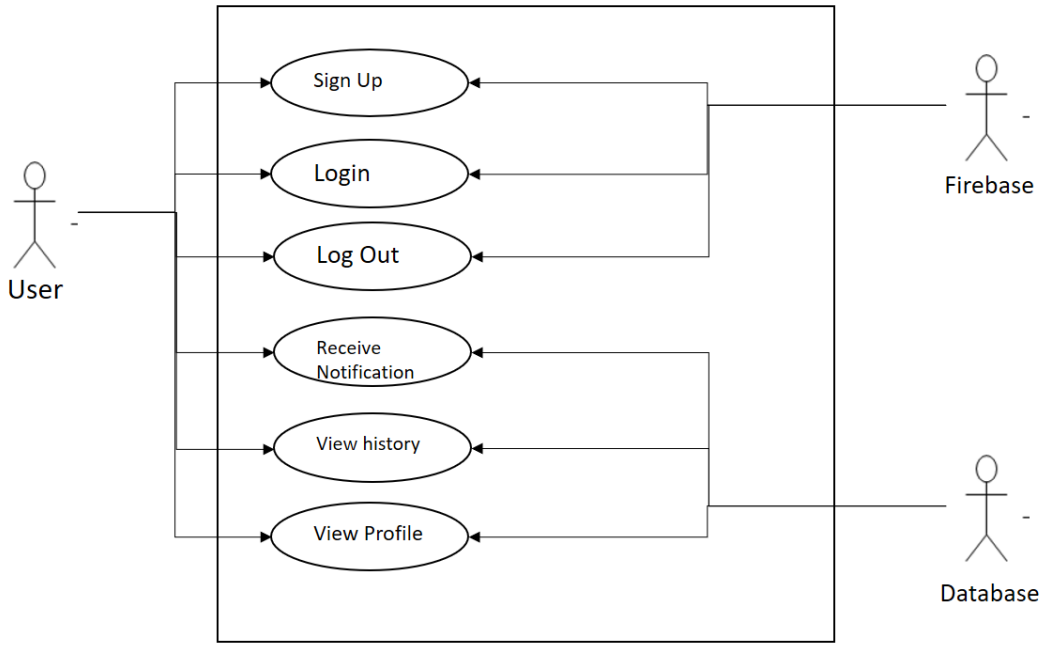

Fig. 5. PSSS mobile application use case diagram.

3. RESULTS AND DISCUSSION

The PSSS was tested with a simulation to determine how the system performs before building a prototype. The simulation provided a fair idea of how the system will work if implemented in a prototype. Proteus® Design Suite 8.8 visual designer was used for the simulation. Figure 6 shows a diagram of the simulation design and Figure 7 shows a diagram of the components to be used in the prototype. The program code was executed on the simulated microprocessor and the electrical circuitry was tested and fine-tuned to produce the best outcome with respect to the system's response.

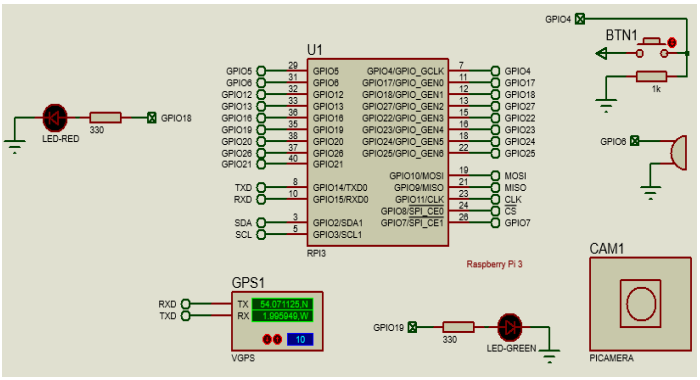

Fig. 6. PSSS simulation diagram.

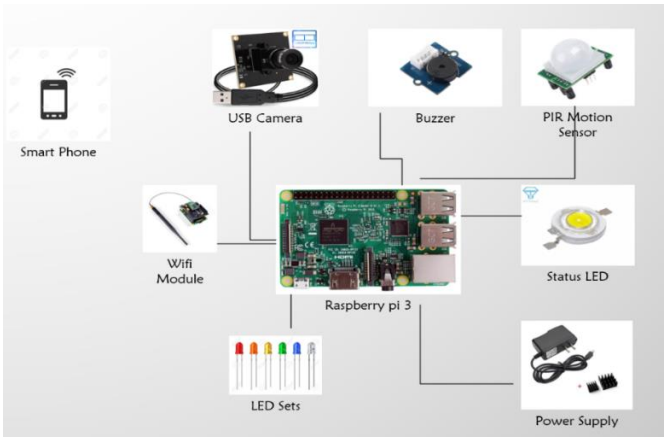

Fig. 7. PSSS proposed prototype build.

Button BTN1 was used to mimic the presence or absence of an intruder. A closed circuit indicates the presence of an intruder. Figure 8 shows a diagram of the button being triggered. When the button is triggered, the buzzer connected to GPIO6 and the LED connected to GPIO18 are activated.

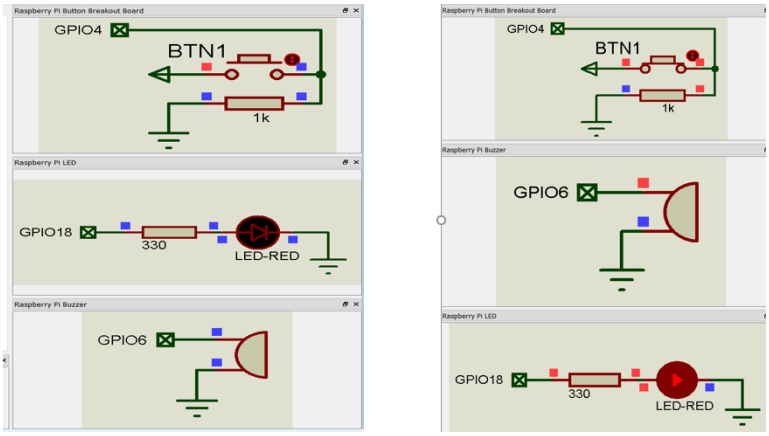

Fig. 8. Button trigger (left: before trigger, right: after button trigger).

3.1. PSSS Mobile Software Application

The mobile software application was developed for Android smart phones. The application was tested to ensure users can sign up, login and receive alert messages. Figures 9 and 10 show images of the application running on an Android device. Aside receiving alerts from current incidents, the user also has the opportunity of viewing a history of alerts. A test account was setup and alert messages were sent to the test account to ensure alert messages were received.

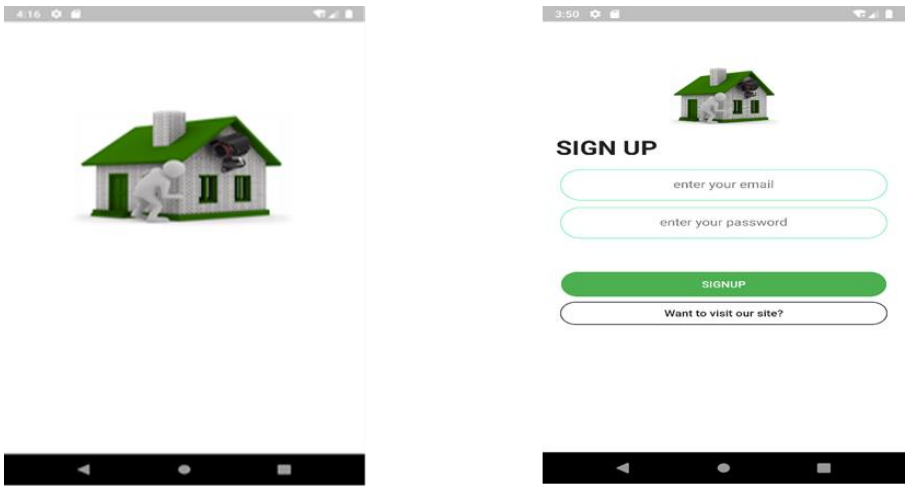

Fig. 9. Application interface (left: splash screen, right: sign up screen).

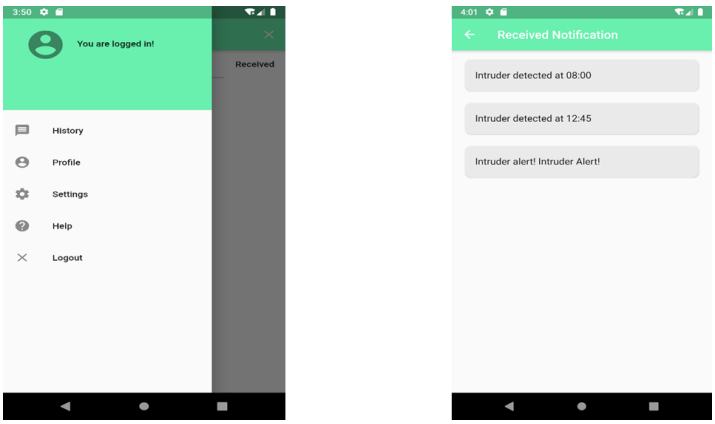

Fig. 10. Application interface (left: menu, right: notification area).

3.2. PSSS Facial Recognition Results

The face recognition algorithm was tested in MATLAB. The **AT&T** dataset of faces [25] was used for initial trials. Further tests involved the use of actual images of persons stored for the purpose of real world tests. Two subjects referred to as Person A and Person B were used to test the algorithm (Figure 11, Figure 12 and Figure 13).

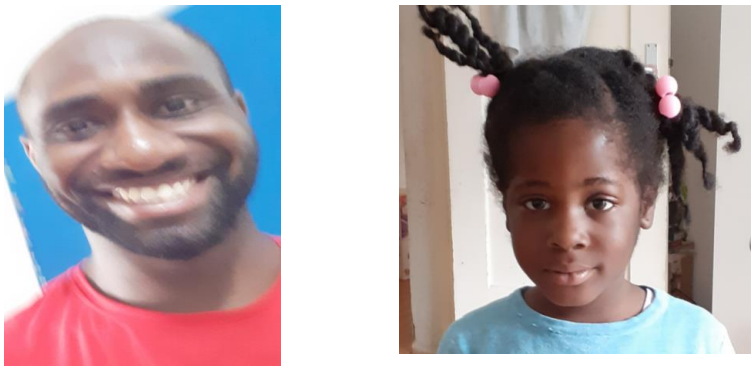

Fig. 11. Person A and B.

The results from the matching and recognition tests both Person A and Person B are shown below.

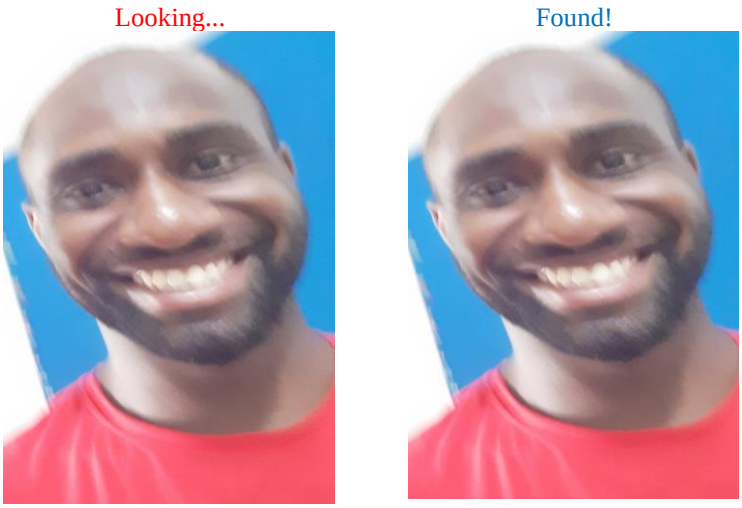

Fig. 12. Matching person A.

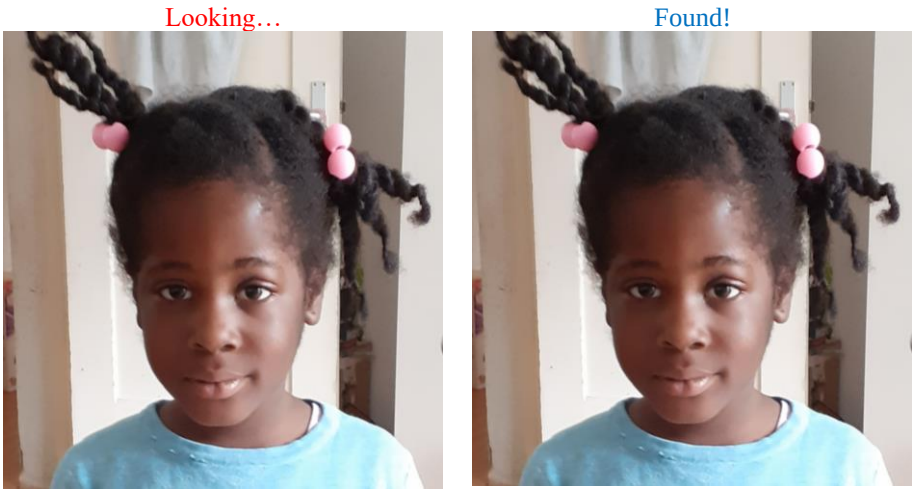

Fig. 13. Matching person B.

The Euclidean distance for each test for person A and person B and the corresponding detection results are shown in Tables 1 and 2. Face recognition tests for Person A were conducted 10 times and for Person B, the number of tests were doubled. A recognition accuracy of 90 % was achieved for both scenarios.

Table 1. Person A Recognition test results (10).

Number	Euclidean Distance	Results	Predicate	
1	0.09	A	positive	
2	0.025	A	positive	
3	0.052	A	positive	
4	0.07	A	positive	9 out of 10
5	0.05	A	positive	90 %
6	0.12	A	positive	Accuracy
7	0.85	unknown	negative	
8	0.67	A	positive	
9	0.36	A	positive	
10	0.74	A	positive	

Table 2. Person B recognition test results (20).

Number	Euclidean Distance	Results	Predicate
1	0.06	B	positive
2	0.05	B	positive
3	0.023	B	positive
4	0.074	B	positive
5	0.62	B	positive
6	0.45	unknown	negative
7	0.27	B	positive
8	0.58	B	positive
9	0.63	B	positive
10	0.74	B	positive
11	0.12	B	positive
12	0.25	B	positive
13	0.69	B	positive
14	0.35	B	positive
15	0.47	B	positive
16	0.54	B	positive
17	0.47	unknown	negative
18	0.46	B	positive
19	0.84	B	positive
20	0.32	B	positive

Testing of the algorithm was also done with different light intensities. The different light intensities provide a fair idea of how face recognition will be done in different lighting conditions. Tests were conducted for night time and day time conditions with different light intensities (high intensity and low intensity). The results of the tests are shown in Table 3 and Table 4. Facial recognition at night was found to be on average 65 % accurate while for day-time conditions it was 85 % accurate.

Table 3. Night time recognition test results.

No. of Attempts	Camera Light Intensities	
	LOW	HIGH
1	detected	detected
2	failed	detected
3	detected	detected
4	failed	failed
5	failed	detected
6	detected	detected
7	detected	failed
8	failed	detected
9	detected	failed
10	detected	detected
11	failed	detected
	6/11	8/11

Table 4. Day time recognition test results.

No. of Attempts	Camera Light Intensities	
	LOW	HIGH
1	detected	detected
2	detected	detected
3	detected	detected
4	failed	detected
5	detected	detected
6	detected	detected
7	detected	failed
8	detected	detected

9	detected	detected
10	failed	detected
11	8/10	detected

The results indicated a high rate of face recognition in the day time and at night when lighting conditions are good. In low light conditions, face recognition performs fairly well. Face recognition can be improved in low light situations by installing high quality lights close to cameras to ensure the cameras are operating in well-lit conditions. Alternatively, low-light cameras can be used to ensure images captured even in low light situations are clear enough for face recognition.

4. CONCLUSIONS

Security is one of the important things for a home. Different methods have been proposed to secure a home with various levels of success. In this paper, we presented a home security system to protect the home from intruders. The proposed system works autonomously without human input. The Private Security Surveillance System (PSSS) is made up of an Area Watch Unit (AWU) which is connected to motion sensors to detect presence of an object and cameras for face recognition if the object is determined to be human. The detected human face is matched to the database to determine if it is a known face and if it is not, an alarm is raised and a message is sent to the home owner's mobile device. A Final Recovery Unit (FRU) is also present in the event that an intruder bypasses or damages the AWU. The FRU raises an alarm and flashes lights to alert of an intruder.

The circuitry of the system was simulated and an Android application was developed to test the functionality of the alert messaging service. Alert messages were received on a test user account created. The facial recognition algorithm was tested using the AT&T dataset of faces. The tests produced an average of 85 % accuracy of the facial recognition algorithm during day time in high and low light intensities. An average of 65 % accuracy was produced in night time conditions. A design for a prototype was proposed and will be built and tested in a real-world situation as part of the future directions.

REFERENCES

[1] https://www.simplypsychology.org/maslow.html. (03 09 2020).
[2] Soumya, S., Chavali, M., Gupta. S., Rao, N., Internet of things based home automation system, IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT, Bangalore, India, IEEE, no. 16583019, 2016.
[3] Abu, M.A., Nordin, S.F., Suboh, M.Z., Yid, M., Ramli, A., Design and development of home security systems based on Internet of Things via Favoriot Platform, International Journal of Applied Engineering Research, vol. 13, no. 2, 2018. p. 1253-1260.
[4] Reddy, G.T., Kaluri, R., Reddy, P.K., Lakshmanna, K., Koppu, S., Rajput, D.S., A novel approach for home surveillance system using IoT adaptive security, Proceedings of International Conference on Sustainable Computing in Science, Technology and Management (SUSCOM), Amity University Rajasthan, Jaipur-India, 2019, p. 1616-1620.
[5] Abdulla, A.I., Abdulraheem, A.S., Salih, A.A., Sadeeq, M.A., Ahmed, A.J., Ferzor, B.M., Sardar, O.S., Mohammed, S.I., Internet of things and smart home security, Technology Report Kansai University, vol. 62, no. 5, 2020, p. 2465-2476.
[6] Vadivukarasi, K., Krithiga, S., Home security system using IOT, International Journal of Pure and Applied Mathematics, vol. 119, no. 15, 2018, p. 1863-1868.
[7] Sultana, T., Wahid, K. A., IoT-Guard: event-driven fog-based video surveillance system for real-time security management, IEEE Access, vol. 7, 2019, p. 134881-134894.
[8] Balla, P.B., Jadhao, K., IoT based facial recognition security system, International Conference on Smart City and Emerging Technology (ICSCET), Mumbai, India, IEEE, no. 18269097, 2018.
[9] Hussein, N.A., Al Mansoori, I., Smart door system for home security using Raspberry Pi3, International Conference on Computer and Applications (ICCA), Doha, UAE, IEEE, no.17287833, 2017.
[10] Ashwini, P., Umale, V.M., Internet of things based home security using Raspberry Pi, Fourth International Conference on Computing Communication Control and Automation, Pune, India, IEEE no.18617925, 2018.
[11] Sarkar, S., Bilgaiyan, S., Android based home security systems using internet of things (IoT) and firebase, Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, IEEE, no. 18357956. 2018.

[12] Bhatia, P., Rajputy, S., Pathakz, S., Prasadx, S., IOT based facial recognition system for home security using LBPH algorithm, International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, IEEE, no. 19453231, 2018.
[13] Kashef, A.E., Barakat, N., Intelligent alarm system to protect small, valuable items, International Conference on Computer and Applications (ICCA), Beirut, Lebanon, IEEE, no. 18095708, 2018.
[14] Suresh, S., Bhavya, J., Sakshi, S., Varun, K., Debarshi, G., Home monitoring and security system, International Conference on ICT in Business Industry & Government (ICTBIG), Indore, India, IEEE, no. 16792091, 2016.
[15] Imran, A., Miah, S., Rahman, H., Bhowmik, A., Karmaker, D., Face recognition using Eigenfaces, International Journal of Computer Applications, vol. 118, no. 5, 2015, p. 12-16.
[16] Sasi, G., Motion detection using passive infrared sensor using IoT, Journal of Physics, Conference Series, vol. 1717, no. 1, 2021.
[17] Mouri, S.P., Sakib, S.N., Ferdous, Z., Taher, A., Automatic lighting and security system design using PIR motion sensor, Journal of Information Technology, Jahangirnagar university, vol. 14, no. 8, 2015, p. 1-5.
[18] Ismail, R., Omar, Z., Suaibun, S., Obstacle-avoiding robot with IR and PIR motion sensors, IOP Conference Series: Materials Science and Engineering, Kuala Lumpur, Malasis, 2016, p. 8-9.
[19] https://cdn-learn.adafruit.com/downloads/pdf/pir-passive-infrared-proximity-motion-sensor.pdf (10.8.2020)
[20] Kaur, R., Himanshi, E., Face recognition using principal component analysis, IEEE International Advance Computing Conference (IACC), Banglore, India, IEEE, no. 15292805, 2015.
[21] Radzi, S.A., Alif, M.M.F., Athirah, Y.N., Jaafar, A.S., Norihan, A.H. Saleha, M.S., IoT based facial recognition door access control home security system using Raspberry Pi, International Journal of Power Electronics and Drive Systems, vol. 11, no. 1, 2020, p. 417-424.
[22] Carıkcı, M., Ozen, F., A face recognition system based on Eigenfaces Method, Procedia Technology, vol. 1, 2012, p. 118-123.
[23] Slavkovic, M., Jevtic, D., Face recognition using Eigenface Approach, Serbian Journal of electrical engineering, vol. 9, no. 1, 2012, p. 121-130.
[24] Perlibakas, V., Distance measures for PCA-based face recognition, Pattern Recognition Letters, vol. 25, no. 6, 2004, p. 711–724.
[25] https://git-disl.github.io/GTDLBench/datasets/att_face_dataset/ (10.08.2020).