IoT Enabled Smart Security Framework for 3D Printed Smart Home

Zhihan Xu
Glasgow College
University of Electronic Science and Technology of China
Chengdu, China
2289012x@student.gla.ac.uk

Shuja Ansari
James Watt School of Engineering
University of Glasgow
Glasgow, United Kingdom
shuja.ansari@glasgow.ac.uk

Amir M. Abdulghani
James Watt School of Engineering
University of Glasgow
Glasgow, United Kingdom
& Smart City Research Group,
Sultan Qaboos University, Oman
amirmohamed.abdulghani@glasgow.ac.uk

Muhammad Ali Imran
James Watt School of Engineering
University of Glasgow
Glasgow, United Kingdom
muhammad.imran@glasgow.ac.uk

Qammer H. Abbasi
James Watt School of Engineering
University of Glasgow
Glasgow, United Kingdom
qammer.abbasi@glasgow.ac.uk

***Abstract*—Recently, smart home design using Internet of Things (IoT) technology has become a growing industry. Since security is the most important element of the smart home design, the project aims to design a 3D printed smart home with a focus on the security features that would meet the security design of futuristic real homes. The surveillance system of traditional smart home is separated from the door lock system. This project innovatively integrates and coordinates them through the facial recognition algorithms, which forms the entry system of this design. The overall system can be divided into two subsystems (parts), which are the sensing and actuation system (PART I) and the entry system (PART II). PART I includes various sensors and actuators to ensure the security of home, including combustible gas sensor, air quality sensor and temperature & humidity sensor. When anomalies are detected by sensors, actuators such as ventilator, buzzer and LEDs start to work. In PART II, the PIR motion sensor is utilized to detect the person to activate the facial recognition step. Facial recognition algorithm (LBPH algorithm) is implemented for person classification, which is used in selecting the duration of recording for the surveillance system. The surveillance system could select not to record for the occupants or different levels of recording for each occupant based on the confidence of recognition. The project outcomes a 3D printed smart home with a door lock system, a surveillance system, and a sensing & actuation network, which accomplishes the security features in perception and network layer of IoT system design.**

Keywords—smart home design, security features, Internet of Things, 3D printing, sensors and actuators

I. Introduction

Smart homes are usually defined as homes with high-tech networks and equipment, which can be remotely accessed, controlled and monitored to improve the convenience of residents [1]. It integrates various services such as security, lighting and heating. Balta-Ozkan et al. [2] think that smart homes have four essential characteristics: a communication network where diverse devices communicate with others; smart controls set to manage the home system; variable sensors equipped to collect the environmental information, which can provide feedbacks from users or sensors.

The IoT is a recent communication paradigm which is a network of interconnected electronic devices [3]. As for layers of an IoT system, it is usually divided into four layers. The first layer is the perception layer which consists of various sensors. The second layer is the network layer which consists of microcontrollers and communication modules. Alireza Zourmand et al. [4] combine LoRa technology and Wi-Fi technology to deploy the IoT system. Nico Surantha et al. [5] utilized Arduino and Raspberry Pi as hardware platform to realize the smart home security system focusing on the object recognition (Person/Non-Person Classification). The third layer is the platform layer. For example, the Ali Cloud is a popular IoT platform which supports LoRa communication. The fourth layer is the application layer which can be a Web or an App.

Since smart home services are diversified, which includes various types of services. Smart security can be divided as two aspects: physical security/safety and data privacy. Most researchers have paid much attention on the data privacy aspect, because devices are usually connected to the Internet and use wireless communication, which provides opportunities for attacks. Zheng et al. [6] note that data security must deal with 3 issues: avoiding data breaches; authorization; ensuring the privacy of the user. However, work presented in this paper mainly focuses on the physical security of smart homes.

In this project, smart home system has been designed with a focus on the security features of the perception layer and network layer that are two bottom layers of an IoT system. The physical devices of the design are divided into three layers. The first layer is the perception layer where various sensors and cameras collect information from the environment. The second layer is microcontroller. Arduino and Raspberry Pi are used in this layer to process data and image, respectively. The third layer is the actuation layer, such as LEDs, ventilator and buzzer.

The structure of the paper consists of six sections. Section 2, 3 and 4 describe the system design method. Section 5 provides results and discussion on the performance of devices and algorithms. Section 6 finally concludes this paper by presenting the project highlights and outcomes.

II. Overall System Design

The proposed smart home system is realized with Arduino Mega2560 and Raspberry Pi 4B. The Raspberry Pi is used due to the low power characteristic of image processing and the Arduino is utilized as the microcontroller to integrate all the electronic components applied in this system. In this section, the overall system design based on the architecture and 3D printing techniques are illustrated.

A. Architecture

Developing the architecture is the first step when designing a system. The overall system is divided into two parts.

One part is the sensing and actuation network inside home, named as PART I. The sensors work constantly to capture the environmental information inside home, such as temperature, humidity and air quality. When anomalies are detected by the sensing network, the actuators will work to alarm and eliminate the anomalies. PART I is shown in Fig. 1.

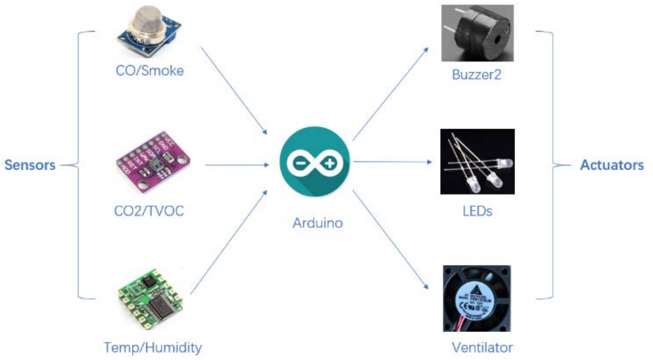


Fig. 1. Sensing and Actuation Network (PART I).

The other part is the entry system of the home, named as PART II, which consists of the door lock system and the Raspberry Pi part. When a person is detected by PIR motion sensor, the camera 1 will be activated to do facial recognition. After successfully capturing image of person's face and performing face recognition (residents or intruders), the door lock system will be activated so that the person can unlock the door by entering the password or fingerprint. After the person successfully unlocks the door, the surveillance system will be activated to record videos by camera 2 according to the confidence of facial recognition. PART II is shown in Fig. 2.

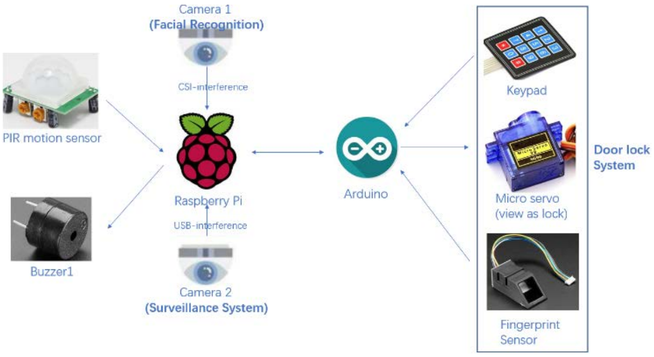


Fig. 2. Entry System (PART II).

The system flowcharts of two parts are shown in Fig. 3 and Fig. 4.

B. 3D Printing

The 3D printing software, Shapr3D, is used in this project. Shapr3D is a professional CAD tool based on IOS system and built for the mobility and precision of the iPad Pro and Apple Pencil [7]. The design details and dimensions are shown in Fig. 5.

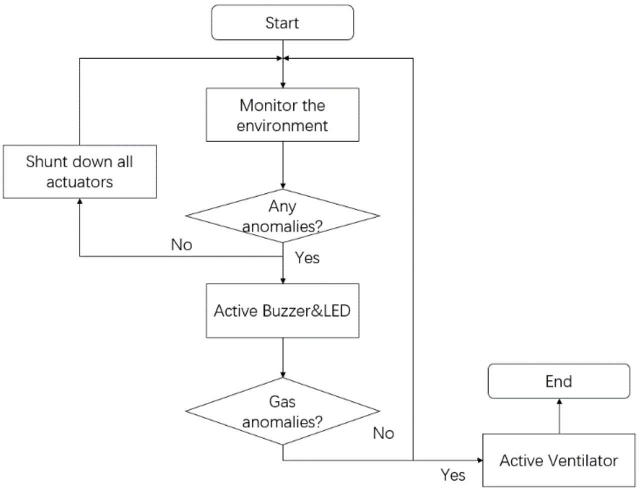


Fig. 3. Flowchart of PART I.

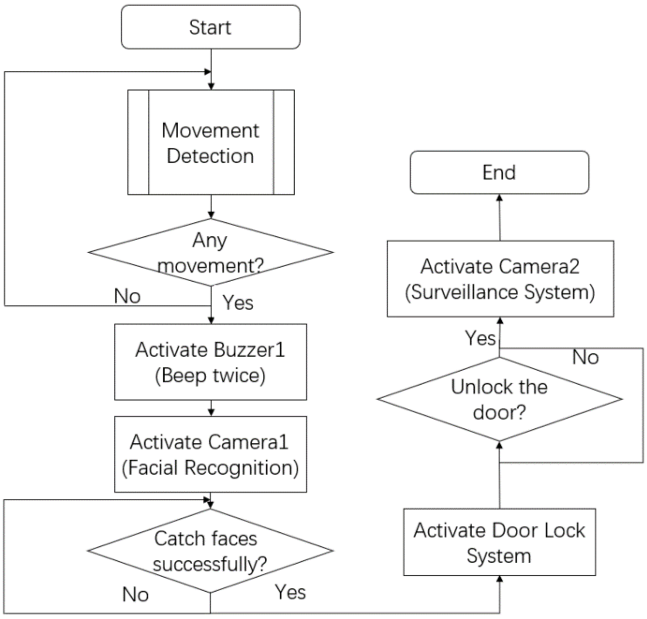


Fig. 4. Flowchart of PART II.

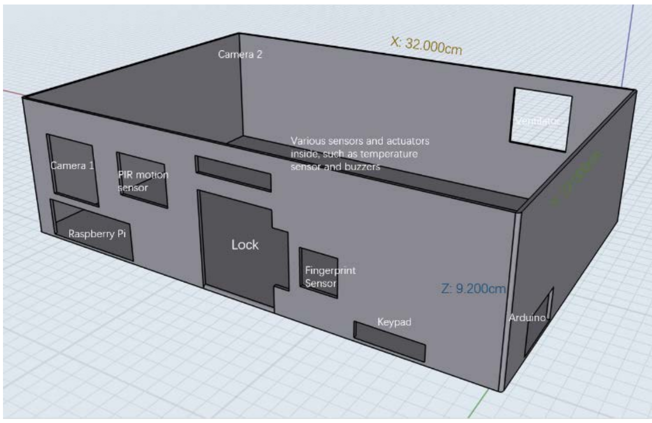


Fig. 5. Design of 3D printed home

III. Hardware System Design

The hardware system design contains the choice of electronic devices and their integration. Table. I below, lists the details of main hardware modules used in this work and their respective descriptions.

TABLE I. MAIN HARDWARE MODULES

No.	Name	Description
1	Arduino	Arduino Mega2560
2	Raspberry Pi	Raspberry Pi 4B for visual processing (facial recognition and surveillance system), with package OpenCV installed
3	Camera 1	CSI-Interference for facial recognition
4	Camera 2	USB-Interference for video recording
5	PIR Sensor	HC-SR501, for movement detection
6	Combustible Gas Sensor	MQ-5, analogue output
7	CO_2/TVOC Sensor	CCS811, I2C communication prototype
8	Temp/Humidity Sensor	Integrated chip SHT20 Detect the temperature and humidity
9	Buzzer 1	Active buzzer connected with Raspberry Pi for notification
10	Buzzer 2	Active buzzer connected with Arduino for alarm
11	Ventilator	12V DC, for improving air quality
12	LEDs	LEDs for notification of anomalies
13	Fingerprint Sensor	Door lock system Component AS608 integrated sensor for fingerprint recognition
14	Keypad	Door lock system Component Total 12 pads, unlock using password
15	Micro Servo Motor	Door lock system Component SG90, viewed as lock
16	Liquid Crystal Display	LCD1602, display the status of home

A. Sensors

Sensors used in this design are Temperature/Humidity sensor, combustible gas sensor, CO_2/TVOC sensor and PIR motion sensor. Only PIR sensor is connected to the Raspberry Pi to detect the existence of person in front of the door. Once the movement is detected, the facial recognition step will be activated. Other three sensors are connected to the Arduino.

Temperature/Humidity sensor is based on the Universal Asynchronous Receiver/Transmitter (UART) communication prototype. Carbon Dioxide (CO_2)/Total Volatile Organic Components (TVOC) sensor is based on I2C communication prototype. The combustible gas sensor uses gas sensitive material tin dioxide (SnO_2). The conductivity of this material increases as the concentration of smoke/Carbon Monoxide (CO) in the air increases. The output is an analogue value ranged from 0-5V, and higher voltages are related to higher concentration of smoke/CO. The analogue-to-digital converter of Arduino is used to view the concentration of the combustible gas.

B. Actuators

Actuators used in this design are buzzers, ventilator and LEDs. Two buzzers are utilized. One is connected to the Raspberry Pi to indicate that facial recognition process has finished. The other is connected to the Arduino to alarm when anomalies happen, for example, air quality getting worse. When the combustible gas concentration rises, the ventilator starts to work. LEDs are connected to Arduino for notification of anomalies.

C. Door Lock System

The door lock system contains a micro servo motor, a keypad and a fingerprint sensor. The micro servo can be viewed as the lock. Its rotation can be viewed as opening or closing of the door. The keypad and fingerprint sensor are used to unlock the door (make the servo rotate) by password and fingerprint, respectively. The Fig. 6 shows working principles of the door lock system.

There are several notes below to illustrate the Fig. 6.

1. The password set in the design is 1234, four digits in total.
2. The unlock process can be activated only when *i=4.*
3. Only clicking 1234 in sequence can unlock successfully. If wrong numbers are clicked, it would be treated it as if the reset button # is clicked, and *i* will be set to 0 again *(i=0).*
4. If unlock successfully, *i* will be set to 0 again *(i=0)*, which is like the reset.
5. * button is used to activate the fingerprint sensor for 10 seconds. If 10 seconds are running out and no correct fingerprints are matched, the door lock system will return to the previous status.

The servo motor is controlled by PWM. The pulse width can determine the rotation angle of the motor. The rotation angle set in the design is 90 degree, so it can be viewed as door's open or close state. Working set and principle of the servo motor is shown in Table. II and Fig. 7 Note that the duration of one period is 20ms.

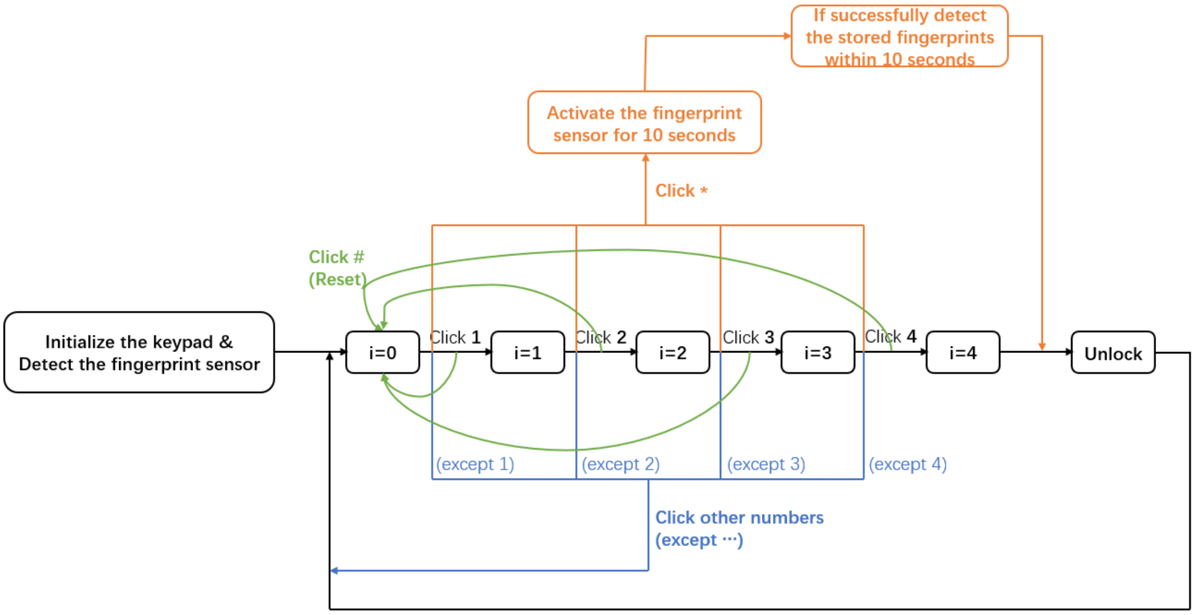

If successfully detect the stored fingerprints within 10 seconds
Activate the fingerprint sensor for 10 seconds
Click *
Click #
(Reset)
Initialize the keypad & Detect the fingerprint sensor
i=0
Click 1
i=1
Click 2
i=2
Click 3
i=3
Click 4
i=4
Unlock
(except 1)
(except 2)
(except 3)
(except 4)
Click other numbers
(except ···)

Fig. 6. Working principles of the door lock system.

TABLE II. WORKING SET OF THE SERVO MOTOR

High-level duration t in the entire period T (20ms)	Rotation angle
0.5ms	0°
1ms	45°
1.5ms	90° (set)
2ms	135°
2.5ms	180°

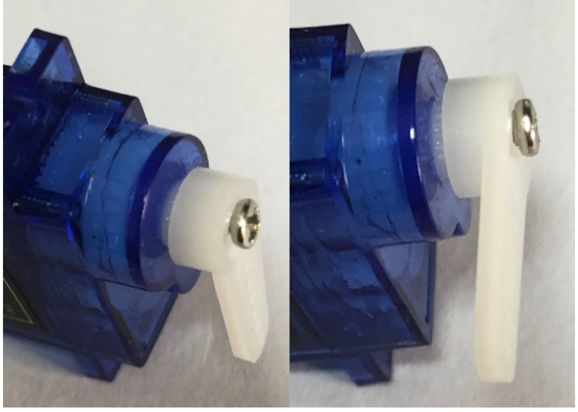
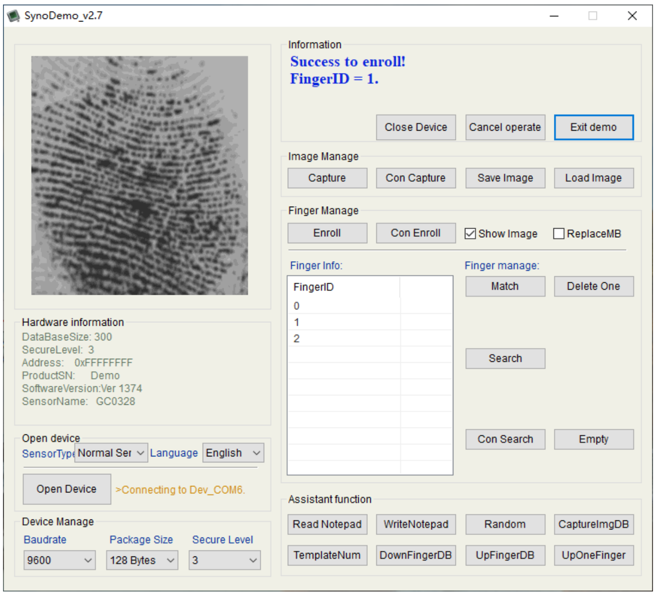


Fig. 7 Working principle of the servo motor (Left: Unlock status, Right: Lock Status).

The keypad used here has 12 pads which are 0-9, * and #. In this design, # button is used to reset in case of misinput and * button is used to activate the fingerprint sensor so that people can also unlock the door using fingerprints.

The fingerprint sensor AS608 used here has a highly powered DSP (Digital Signal Processing) chip which can render images, perform calculations and find features [8]. A total of 162 fingerprints can be stored in the onboard FLASH memory [8]. The software SynoDemo shown in Fig. 8 is used to enrol the fingerprints with IDs.



SynoDemo_v2.7

Information
Success to enroll!
FingerID = 1.

Hardware information
DataBaseSize: 300
SecureLevel: 3
Address: 0xFFFFFFFF
ProductSN: Demo
SoftwareVersion:Ver 1374
SensorName: GC0328

Open device
SensorType: Normal Ser
Language: English
>Connecting to Dev_COM6.

Device Manage
Baudrate: 9600
Package Size: 128 Bytes
Secure Level: 3

Finger Info:

FingerID
0
1
2

☑ Show Image
□ ReplaceMB

Fig. 8 Interface of the SynoDemo.

D. Others

The LCD1602 is used to display the current status of home. There are 6 statuses shown in Table. III below.

TABLE III. STATUSES OF HOME

Status #	Explanation
1	Monitoring the environments
2	Motion Detected (Face Recognition Activated)
3	Face Recognition Finished (Door Lock System Activated)
4	Password Correct, Unlock Successfully (Surveillance System Activated)
5	Fingerprint Sensor Activated
6	Fingerprint Detected, Unlock Successfully (Surveillance System Activated)

IV. Software System Design

This software design focuses on the Raspberry Pi part (PART II). In this section, the details and process of facial recognition are illustrated. How the surveillance system works is also provided.

A. *Facial Recognition*

The facial recognition algorithm can be divided into three steps shown in Fig .9. Firstly, gather face images (data) of the person to be identified. This step needs to set an ID for each image so that the algorithm can recognize an input image according to it. Secondly, feed all face images and their respective ID's to the recognizer so that it can learn. Finally, the recognizer works and give feedback of confidence.

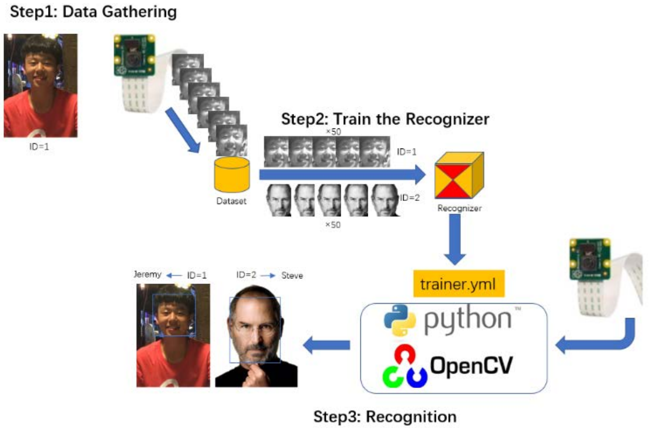


Fig. 9. Facial Recognition Steps

Note: The picture of Steve Jobs in this paper is not for commercial use.

1) *Data Gathering*

The first step aims to create a dataset with face images and their respective IDs. It is noteworthy that all images are transformed into grayscale for further training. The face classifier used is haarcascade_frontalface_default.xml [8] which can detect faces in an image. The number of IDs equals to the number of occupants for the home. In this design, the number of IDs or occupants is 2 (Jeremy & Steve). Each ID will store 50 samples or faces for training.

2) *Train the Recognizer*

The recognizer used in this design is Local Binary Pattern Histograms (LBPH) provided in the OpenCV library, which is a popular face recognition algorithm. To explain the LBPH, brief introduction to Local Binary Pattern (LBP) operation has been presented first.

LBP is an efficient texture operator which labels pixels of an image by thresholding the surrounding pixels (0 or 1) of each pixel and then concatenates the results in a defined way as a binary number [9]. Steps of basic LBP shown in Fig. 10 are defined as follows:

1. Suppose there is a face image represented in grayscale.
2. Get part of the image with a window of 3×3 pixels (The intensity ranges from 0 to 255 of each pixel).
3. Take the central pixel intensity value as the threshold.
4. For each surrounding pixel value, mark as 1 for values equal or larger than the threshold, otherwise 0.
5. Concatenate each surrounding binary value in clockwise or anticlockwise direction.
6. Convert the binary value to the decimal value known as the LBP value, and set it to the central value which describes the texture information of this area.

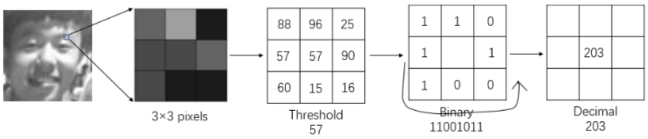


Fig. 10. Steps of Basic LBP

After the LBP procedure, a new image with better feature representations of the origin image is obtained. However, the covering area is a big flaw of the basic LBP operator because of the fixed radius, as it cannot meet the requirements of diverse sizes and frequency textures. To solve this problem, Ojala et al. [10] improved the LBP operator by replacing the square window with the circular neighbourhood with a non-fixed radius, which extends the covering area to any neighbourhood. The LBP operator containing P sampling points in a circular area of radius R is got, which is called circular LBP operator. The Fig. 11 shows circular LBP examples below.

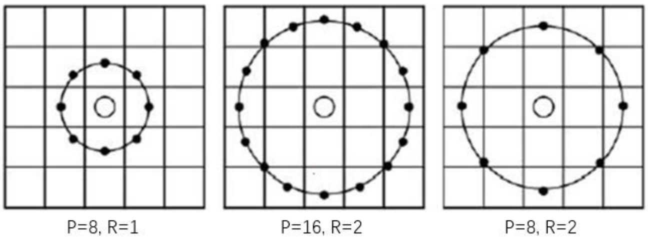


Fig. 11. Circular LBP Examples

As for LBPH, one more step of extracting the histograms works on the image generated by LBP step. The image is divided into grids. Each grid corresponds to a histogram with 256 positions (0~255), which can represent the occurrences of each pixel intensity. Then, concatenation of each histogram is done to obtain a new and bigger histogram for the original image. For example, if having 6×6 grids, there will be 6×6×256=9216 positions in the final histogram, representing the features of the original image. Details are depicted in Fig. 12.

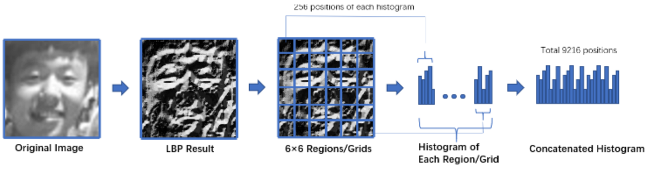


Fig. 12. Extracting the Histograms

3) *Recognition*

As for recognition, the key is comparing the histograms between two images by calculating the distance between two histograms. There are various methods, such as Euclidean distance, chi-square, and absolute value. For example, Euclidean distance D defined as the following formula where n is the total positions of concatenated histogram. The algorithm will return the calculated distance which is inversely related with the confidence.

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

B. *Surveillance System*

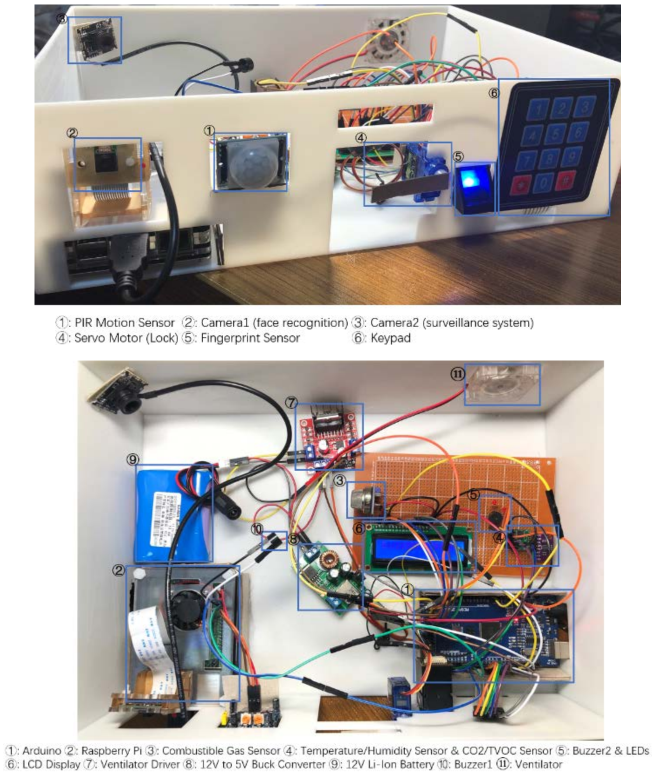
The time duration of video recording depends on the confidence of the recognition. In order to improve the trust-level, the average-value method was adopted. After successfully recognizing an occupant for 10 times, the program will calculate the average confidence of these 10 values. If the average is larger or equal to 50%, the surveillance system will not record videos. If the average is between 30% to 50%, the system will record videos for 10 minutes. If the average is less than 30%, the system will record videos for 30 minutes. However, if the system recognizes the person as “unknown” (negative value), it will record videos constantly. Detailed operation mechanism of the surveillance system is shown in the Table 2 below.

TABLE IV. MECHANISMS OF SURVEILLANCE SYSTEM

Average Confidence	Time Duration of Video Recording
>50%	No recording
30%~50%	10 minutes
0~30%	30 minutes
<0 (“unknown”)	Constantly

V. RESULTS AND DISCUSSION

In this section, the results of the entire system are presented and discussed, and potential further work is also deliberated. The entire final design is shown in Fig. 13. As illustrated in section 2, the overall system can be divided into two subsystems which are sensing and actuation network (PART I) and the entry system (PART II).



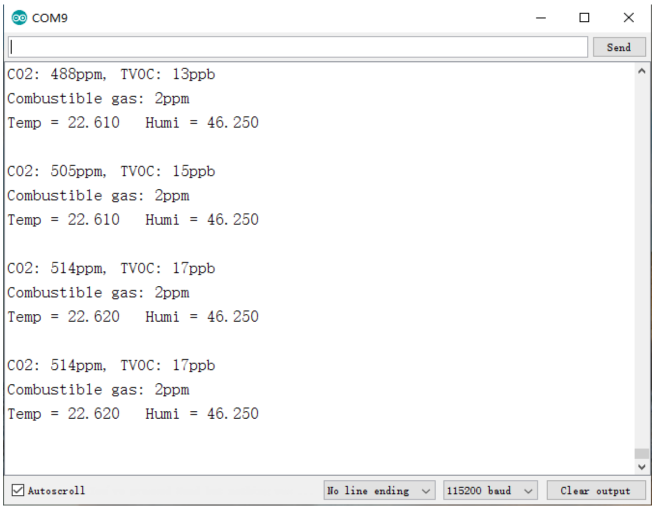
①: PIR Motion Sensor ②: Camera1 (face recognition) ③: Camera2 (surveillance system)
④: Servo Motor (Lock) ⑤: Fingerprint Sensor ⑥: Keypad

①: Arduino ②: Raspberry Pi ③: Combustible Gas Sensor ④: Temperature/Humidity Sensor & CO2/TVOC Sensor ⑤: Buzzer2 & LEDs
⑥: LCD Display ⑦: Ventilator Driver ⑧: 12V to 5V Buck Converter ⑨: 12V Li-Ion Battery ⑩: Buzzer1 ⑪: Ventilator

Fig. 13 Final design outcome (front view & top view)

As for the sensing and actuation network (PART I), the result is shown in Fig. 14. From the result, it is easy to find the environmental information of the home, including the temperature, humidity and air quality.

As for the entry system (PART II), the results are twofold. For one, the result of the door lock system is shown in Fig. 15. From the figure, it is easy to identify the way (Fingerprint or Password) a person used to unlock the door. If using the fingerprint, the ID of the fingerprint and confidence are also shown. For the other, the result of facial recognition shown in Fig. 16. The algorithm works by capturing the image of the face and giving the feedback of the confidence.



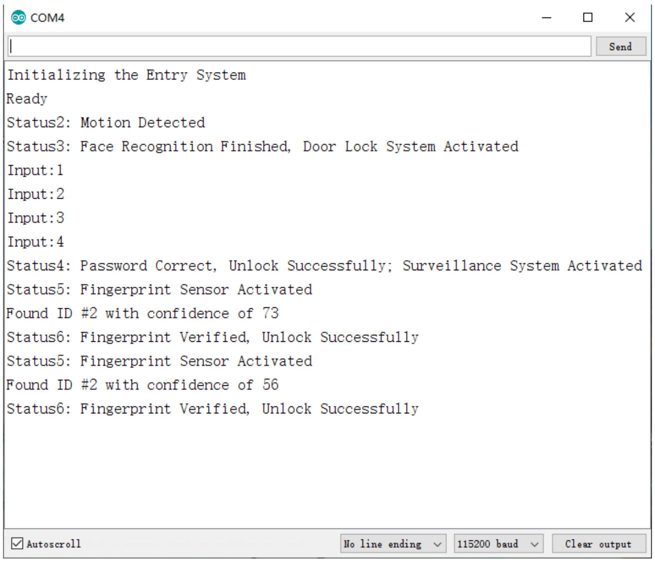
```
CO2: 488ppm, TVOC: 13ppb
Combustible gas: 2ppm
Temp = 22.610    Humi = 46.250

CO2: 505ppm, TVOC: 15ppb
Combustible gas: 2ppm
Temp = 22.610    Humi = 46.250

CO2: 514ppm, TVOC: 17ppb
Combustible gas: 2ppm
Temp = 22.620    Humi = 46.250

CO2: 514ppm, TVOC: 17ppb
Combustible gas: 2ppm
Temp = 22.620    Humi = 46.250
```

Fig. 14 Result of the sensing and actuation network (PART I).



```
Initializing the Entry System
Ready
Status2: Motion Detected
Status3: Face Recognition Finished, Door Lock System Activated
Input:1
Input:2
Input:3
Input:4
Status4: Password Correct, Unlock Successfully; Surveillance System Activated
Status5: Fingerprint Sensor Activated
Found ID #2 with confidence of 73
Status6: Fingerprint Verified, Unlock Successfully
Status5: Fingerprint Sensor Activated
Found ID #2 with confidence of 56
Status6: Fingerprint Verified, Unlock Successfully
```

Fig. 15 Door lock system result of the entry system (PART II).

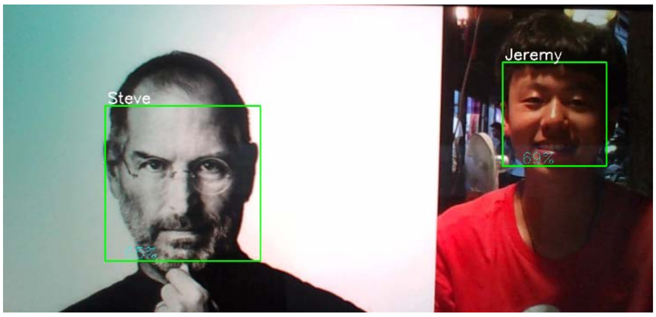


Fig. 16 Facial recognition of the entry system (PART II).

Note: The units of the temperature and humidity in Fig.14 are °C and %RH, respectively.

In the future, other facial recognition algorithms can be tried, since the LBPH algorithm cannot achieve very high confidence (higher than 80%) and is sensitive to the light condition, although the LBPH algorithm can meet the needs of smart home design. For example, the FisherFace algorithm based on Linear Discriminant Analysis (LDA) is also a popular method of facial recognition [12]. It is also included in the OpenCV package. Additionally, the Dlib library is also popular in the implementation of facial recognition, which uses the Hog features of image to represent faces.

VI. Conclusions

In this project, a 3D printed smart home with a focus on security features is designed. It is an entire innovative engineering process involving electronics, hardware prototyping and machine learning. The proposed system integrates Raspberry Pi 4, Arduino, cameras and various sensors & actuators. The overall system can be divided into two subsystems which are sensing and actuation network (PART I) and entry system (PART II). The sensing and actuation network can monitor the environment of the home and give feedbacks when anomalies happen. The novelty of the design is the entry system which integrates and coordinates the door lock system and the surveillance system through the facial recognition algorithms. Residents can unlock the door using fingerprints or password only after the completion of face recognition process. The result or confidence of facial recognition algorithms will directly determine the working duration of the surveillance system which can be activated only when the door is successfully unlocked. The system meets the basic security requirements of smart home design in real world and realizes the perception layer and network layer of an IoT system which lays foundations for further platform layer and application layer design.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestions and comments on this paper. This work is supported by the Glasgow College, University of Electronic Science and Technology of China.

References

[1] Marie Chan, Daniel Estève, Christophe Escriba, Eric Campo, "A review of smart homes—Present state and future challenges," *Computer Methods and Programs in Biomedicine*, Volume 91, Issue 1, Pages 55-8, 2008.

[2] Nazmiye Balta-Ozkan, Rosemary Davidson, Martha Bicket, Lorraine Whitmarsh. "The development of smart homes market in the UK," *Energy*, Volume 60, Pages 361-372, October 2013.

[3] Chii Chang, Satish Narayana Srirama, and Rajkumar Buyya. 2018. "Internet of Things (IoT) and New Computing Paradigms," In *Fog and Edge Computing: Principles and Paradigms.* Wiley Press, New York, USA, Chapter 1. In Press.

[4] A. Zourmand, A. L. Kun Hing, C. Wai Hung and M. AbdulRehman, "Internet of Things (IoT) using LoRa technology," *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, Selangor, Malaysia, pp. 324-330, 2019.

[5] Nico Surantha, Wingky R. Wicaksono, "Design of Smart Home Security System using Object Detection and PIR Sensor, " *Procedia Computer Science*, Volume 135, Pages 465-472, 2018.

[6] Y. Zheng *et al.*, "Unobtrusive Sensing and Wearable Devices for Health Informatics," in *IEEE Transactions on Biomedical Engineering*, vol. 61, no. 5, pp. 1538-1554, May 2014.

[7] Shapr3D: The World's Leading Mobile 3D Design App for iPad. [Online] Available: https://www.shapr3d.com/

[8] Grove – Fingerprint Sensor. [Online] Available: http://wiki.seeedstudio.com/Grove-Fingerprint_Sensor/

[9] Open Source Computer Vision Library, haarcascade_frontalface_default.xml [Online] Available: https://github.com/opencv/opencv/tree/master/data/haarcascades

[10] T. Ahonen, A. Hadid and M. Pietikainen, "Face Description with Local Binary Patterns: Application to Face Recognition," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037-2041, Dec. 2006.

[11] T. Ojala, M. Pietikainen and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971-987, July 2002.

[12] Mustamin Anggo and La Arapu, "Face Recognition Using Fisherface Method" *Journal of Physics: Conference Series*, vol. 1028, Jun. 2018.