

Development of a Facenet Enhanced Secured Smart Office System

Odeyemi C. S.*

Computer Engineering Department, Federal University of Technology, Akure, Nigeria

E-mail: charityodeyemi@gmail.com; csoyeyemi@futa.edu.ng

ORCID iD: <https://orcid.org/0000-0002-1160-9394>

*Corresponding author

Olaniyan O. M.

Department of Computer Engineering, Federal University, Oye Ekiti, Nigeria

E-mail: olatayo.olaniyan@fuoye.edu.ng

ORCID iD: <https://orcid.org/0000-0002-7349-7500>

Received: 28 October 2023; Revised: 27 November 2023; Accepted: 15 December 2023; Published: 08 February 2024

Abstract: A secured smart office system is the one that is capable of recognizing and granting access to authorized persons only and manage the office appliances autonomously. The goals are access control, security and automation. Over the years, several studies have been carried out to meet these needs using RFID cards, access codes and biometrics resulting in weak security with long computational period. Switching of electrical appliances and smoke detection in case of fire outbreak were used but real time electrical appliances management that could prevent fire outbreak is yet to be achieved. This research focused its attention on the design and implementation of a smart office system that meet these needs. The system was developed using a raspberry pi 4 board. Ultrasonic sensor, camera, servo motor, relay, current and voltage sensors were interfaced with the raspberry pi for image capturing, opening the door, switching and power monitoring respectively. The system captures the image of an approaching person and process it for recognition using FaceNet; an open source model for face recognition. Information was transmitted via SIM800L GSM module as SMS to the administrator. The system shuts down the office electrical network once the supply voltage exceeds 220v ac or less than 161v ac, thus preventing any chance of fire outbreak due to irregular power supply. The accuracy of image recognition model was 93.13%. This research has shown a simple way of implementing an autonomous smart office system that is capable of providing adequate security, efficiency and convenience in offices.

Index Terms: Access Control, FaceNet, Office Automation, Raspberry pi, Security, Smart.

1. Introduction

A smart office uses cutting edge technology to ensure convenience and security for smooth and seamless running of an organization. One of the main challenges of an organization's administrative office is access control and security of information and systems. Also, growth in organizational and business structures as well as advancement in technology necessitate improvement in office security. Therefore, very strong security measures must be in place to prevent damages and loses in the organization as a result of unauthorized access and fire outbreak. This must be done by implementing a technology that ensures accuracy, safety and very convenient to use in other to enhance an efficient running of the office [1]. This prompts the need for a fast deep learning based office environment for solving the problem of access to authorized persons. That is a secured but smart system which is able to discriminate quickly and accurately between the office user and an intruder; and prevent fire outbreak in the offices. Also, because of the rapid expansion in semiconductor devices which are the building block of most office appliances and the need for energy management; embedded systems and automation with wireless communication for simple management of electrical appliances have emerged as important components of technological advancement [2, 3]. Consequently, smart systems have become essential areas of research in recent years as a result of the benefits it has provided to the world of technology as well as a source of comfort to humanity [4]. Smart systems provide means of managing several appliances from a single area rather than going to each one's individual control points or switches [5, 6]. However, because of the need for security and access control, recent studies in office automation have expanded to including face recognition for access control. Face recognition is a non-contact and non-intrusive method of biometric identification. It

maps human facial features from a digital image and match it with the database of images for the purpose of authenticating the identity of the office user. It works by using computer generated filters to transform facial images into numerical expressions that can be compared to determine their similarities [6]. Every face has numerous, distinguishable features or landmarks, these are the different peaks and valleys that make up facial features. Each human face has approximately 80 distinguishable features [6-9]. Some of the features measured by software are:

- Distance between the eyes.
- Width of the nose.
- Depth of the eyes socket.
- The shape of the cheekbones.
- The length of the jaw line

These features are measured creating numerical code representing the face in the database [6,7]. The process is as shown in figure 1.

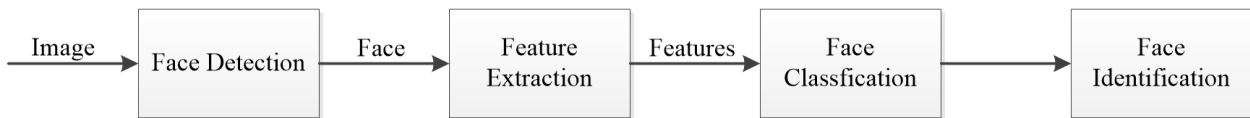


Fig.1. Block diagram representing the process of face recognition



Fig.2. The architecture of FaceNet [10]

Among the face recognition models available, FaceNet developed by Google research team in 2015 stands out as a state of the art face recognition, verification and clustering neural network. It uses deep convolutional neural network (CNN) by mapping facial features into Euclidean space where distances directly correspond to how similar the faces are. The faces are therefore compared with the space thus able to infer whether they are the faces of the same person or not. Therefore, FaceNet whose architecture is shown in Figure 2, learned a compact embedding space where face images of the same identity are close together and dissimilar faces are far apart. It is used in transfer learning by training the network on a large-scale dataset and fine-tuning it on the face recognition task [11-14].

The system therefore grants access only to the person whose face is recognized. A smart office is an office environment that can make decisions autonomously [7]. It should be able to recognize and decide who can and who cannot enter the room and when the electrical appliances are needed. Most of the fire accidents that usually occur in the offices are electrical in nature. This is usually as a result of an abnormality or irregularity in the public electric power supply as being experienced in Nigeria and other developing countries of the world [12]. The smart office will be equipped with devices that will prevent fire outbreak with real time information transmission to the person in charge.

2. Related Works

There have been studies previously done on smart office design, some of these studies were keenly reviewed before embarking on this design. The review discussed the methods used by various researchers, results obtained and the weaknesses discovered.

Bhuyar and Ansari [7] designed and implemented a smart office automation system which uses sensors to extract the real time data from environment and feed to the ARM 11 controller for processing to control the fan, bulb and the

buzzer connected to the controller. These output signals activated devices when the system crosses the preset or threshold value. However, no provision was made for the prevention of fire outbreak and access control. In research into smart office for monitoring and control appliances, Shaikh and Kapare [8] designed a prototype system which can be implemented for surveillance and control of electrical appliances in an office on the world-wide-web. The proposed system was designed to use a smartphone through Bluetooth and Raspberry pi as communication protocol and server respectively. This research proposed a designed, though not implemented which aimed at controlling electrical appliances online but makes no provision for office user identification and security. Prototype smart office security system was developed by Prasetyo, Zaliluddin and Iqbal [9] using IoT which was modelled on cayenne platform; thus, the data could be accessed and the office devices controlled over the internet network. The prototype was built using arduino mega 2560 microcontroller. It was able to detect threats of dangerous metallic objects and bang on the door or floor but made no provision for access control or the conveniences of the office user. Research into a smart office with face detection focusing on edge computing paradigm to process data locally in which its closeness to the user helped to avoid the problem of slow communication of data to centralized datacenters. In this paper Prentice and Karakonstantis [10] developed and evaluated an end to end office application on a representative edge device, Raspberry-pi, while utilizing cloud on demand services connected through an Android application and Amazon Alexa Skill. The system monitored several environmental conditions and is able to recognize users by facial recognition. However, the work was limited to recognition; no system of control was included.

Previous designs using biometric authentication were only able to make weak authentication of the regular office user(s) because of their low accuracy and long computation period, the office user is sometimes detected as an intruder [11]. Smoke and gas sensors used in previous studies were able to detect fire after it has occurred but could not prevent it. In other to overcome these problems, this paper presents a prototype low cost and simple smart office system designed to recognize, grant access to the office user and have alternative means of granting access to a non-regular office user but who is authorized to enter. It was equipped with sensors capable of detecting irregularities in the power supply which is the main source of fire outbreak in offices [1] and prevent the fire by switching off the supply until normality is restored. These together with information on appliances switching were transmitted on real time to the admin's phone as SMS.

3. Research Context and Methodology

The research methodology focused on the observed gap in the previous studies. Office security consists of both effective access control and protection of the appliances. This section consists of block diagram and electrical circuit design, fabrication, software integration and system testing.

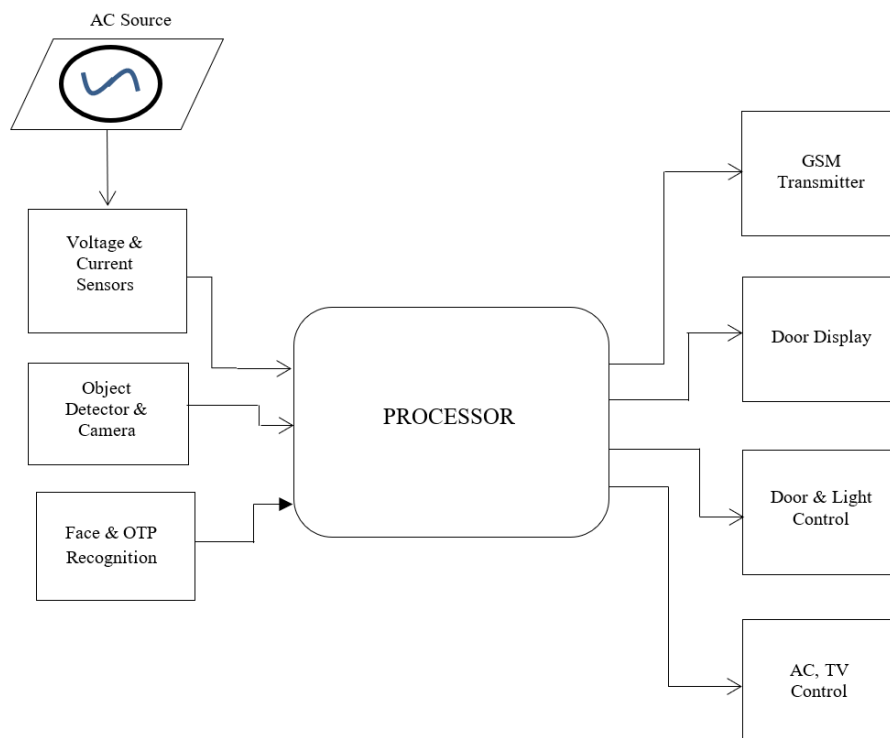


Fig.3. The block diagram of the secured smart executive office system

3.1. The Circuit Design

The complete system circuit design was carried out based on the block diagram shown in Figure 3. The voltage sensor, current sensor, ultrasonic sensor and camera were interfaced with the processor to perceive the office environment and send the data to the processor for storage, analysis, processing and decision making. Connections were made to the processor so that the output of the processor send signals to the switches and relays as actuators to control the door, light bulbs, TV, AC and electrical power distribution board [12,14]. A GSM module was interfaced with the processor thus providing a communication network for transmission of information about the activities in the office as a short message system (SMS) to a remote mobile phone [14-16].

The circuit design was done on Proteus 8.0 Professional, an open source software for engineering design [17]. The designed circuit which incorporates all the circuit element/components of the research is as shown in figure 4.

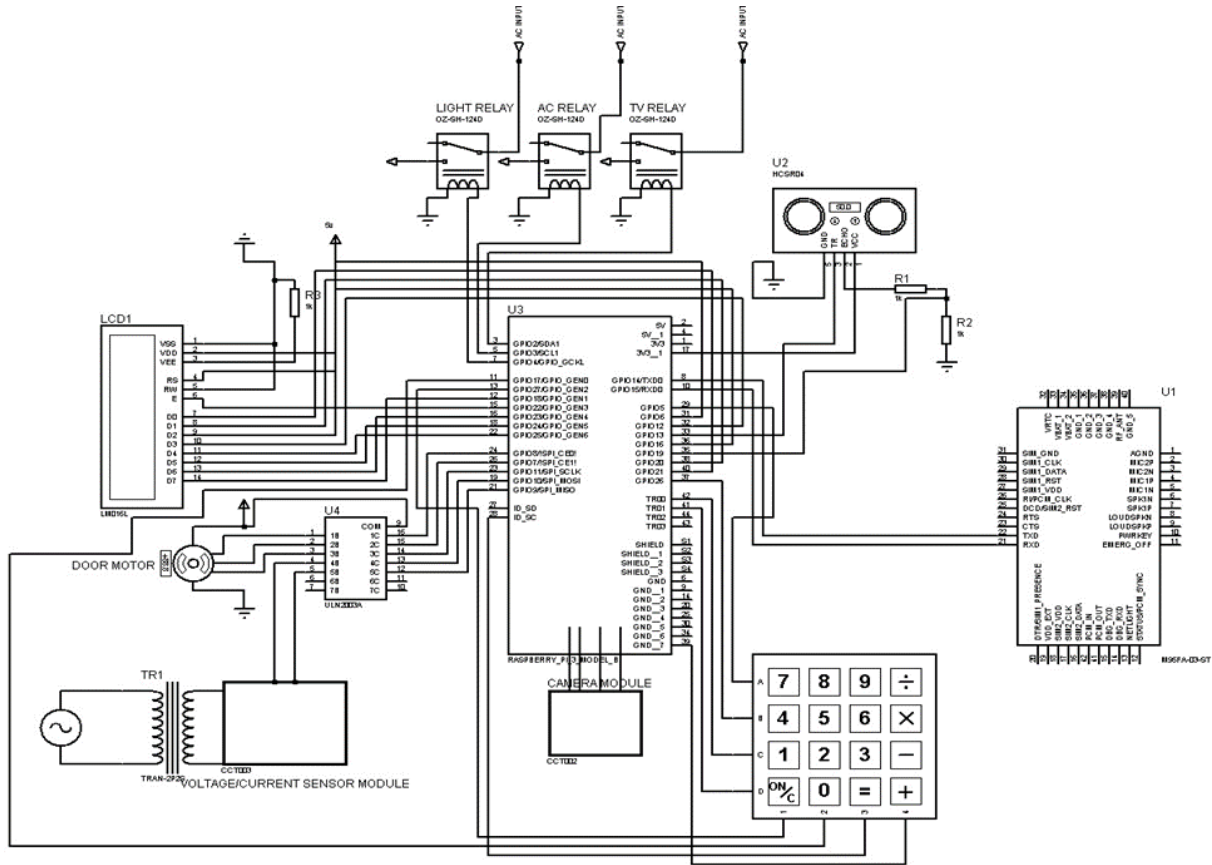


Fig.4. The complete circuit diagram of the smart executive office system

The system design was implemented as a hardware prototype driven by software.

3.2. The Power Supply Unit

The system was powered by four 5v 18650 lithium batteries connected in parallel and being charged by a TP4056/TC4056A Lithium battery charger and protection module as shown in figure 5. Each 18650 lithium battery is rated 5v, 2200mAh, since the total voltage in a parallel circuit is the same value as the voltage across each branch [18];

$$V_T = V_1 + V_2 + V_3 + V_4 \tag{1}$$

The total current in a parallel circuit is the sum of the individual branch currents;

$$I_T = I_1 + I_2 + I_3 + I_4 \tag{2}$$

Applying equations (1) and (2) to the connection in Figure 5, the effective rating of the cells is 5v, 8800mAh which makes the system last long whenever there is power outage from the public supply.

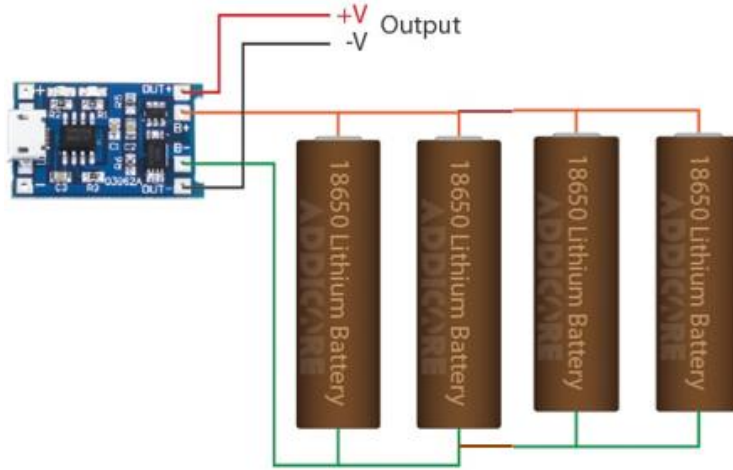


Fig.5. Power supply unit

The details of the specification of the battery charger are as shown in Table 1.

Table 1. Lithium battery specifications [18-20]

FEATURES	SPECIFICATIONS
Charge Controller	TP4056 / TC4056
Protection IC	DW01A
Charge/Discharge Control MOSFET	FS8205A
Charge Method	Constant-Current/Constant-Voltage (CC/CV)
Input Supply Voltage	4.5~6.0 V
Constant Charge Current	1 A Configurable with Rprog resistor
Charge Complete (Float) Voltage	4.2 V \pm 1.5%
Overcharge Detection Voltage	4.3 V \pm 50 mV
Overcharge Release Voltage	4.1 V \pm 50 mV
Over-Discharge Detection Voltage	2.4 V \pm 100 mV
Over-Discharge Release Voltage	3.0 V \pm 100 mV
Overcurrent Protection Threshold	3 A
Short-Circuit Cutout Delay	5~50 μ s
Trickle Charge Threshold Voltage	2.9 V \pm 0.1 V
Trickle Charge Current	130 mA \pm 10 Ma

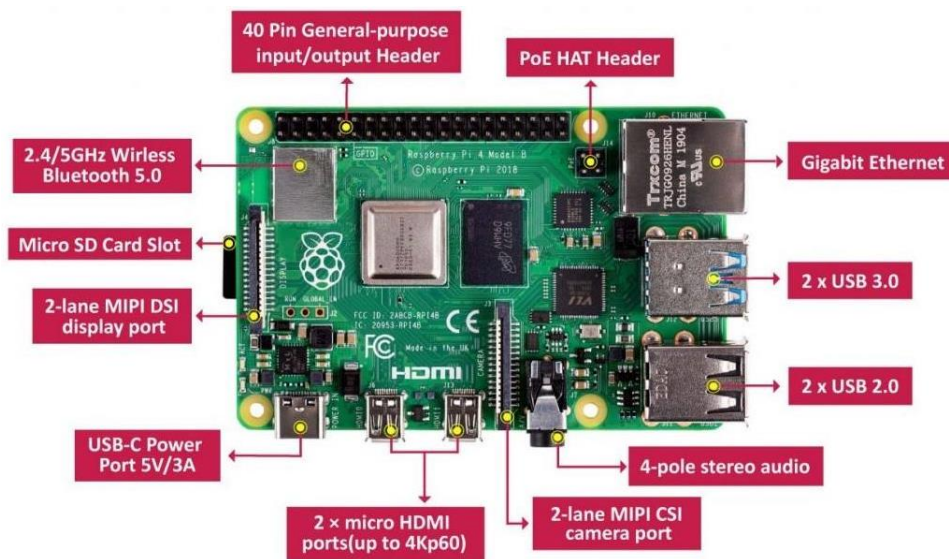


Fig.6. Architecture of BCM2711 processor [4]

3.3. The Processor: BCM2711

The BCM2711 processor whose architecture was shown in Figure 6 was used for this research. It is an upgraded form of the 64-bit quad-core SoC design. It uses a powerful ARM A72 core, very fast input/output GPU features and an Ethernet controller [4,17-20]. It is used on Raspberry pi-4 boards upon which the research was built.

3.4. Hardware Fabrication

The designed system was fabricated on circuit board, firmly connected and the image of the completed work is shown in Figure 7. The connections which were made on the vero-board was firm and rigid, the arrangements also allow for easy mount on the chassis.

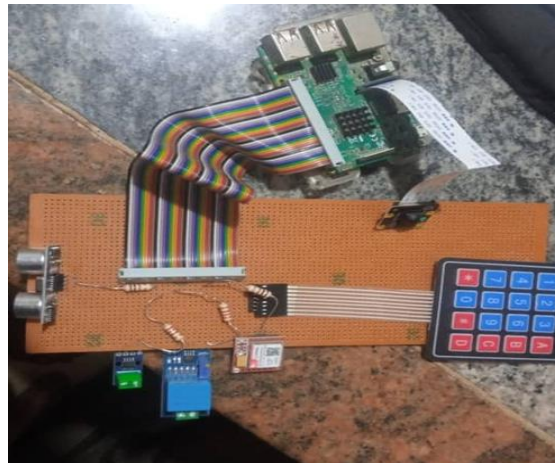


Fig.7. Assemblage of the hardwares

3.5. Control Software

This research made use of a custom software developed on python IDE into which a trained open source model; FaceNet (for image classification) was imported as the control software for the system. FaceNet, a popular transfer learning model for facial recognition was employed which embeds the input images into a 128 dimensional vector encoding as shown in Figure 7.

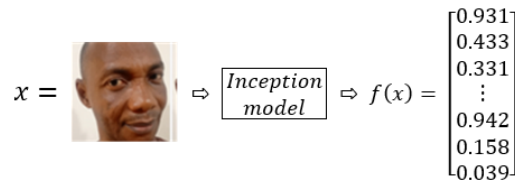


Fig.8. Process of features extraction and embeddings generation

Therefore, it was trained to adapt the model to the dataset (images) for this study. The pre-trained model's labels were modified to reflect the new task, unused layers frozen and the new data files uploaded to train with [10, 13-14]. The FaceNet model was then trained on triple loss function shown in equation 3. Triple loss function helps the model to learn embeddings that enhance the similarity between images of the same identity and maximize the dissimilarity between images of different identities.

$$Loss = \sum_{i=1}^N [\|f_i^a - f_i^p\|_2^2 - \|f_i^a - f_i^n\|_2^2 + \alpha] \tag{3}$$

where:

- a = anchor embedding (original image)
 - p = positive embedding (another image of 'a')
 - n = negative embedding (different image from 'a')
- based on Euclidean distance and hyperparameter that defines the desired separation between the positive and negative [6, 10].

During training, the model's weights were updated using gradient descent optimization to minimize the triplet loss. The gradient descent optimization function is shown in equation 4

$$a_{n+1} = a_n - \gamma \nabla F(a_n) \tag{4}$$

where:

a_{n+1} = new weight

a_n = old weight

γ = learning rate

$\nabla F(a_n)$ = gradient of the loss with respect to the weight [10]

Three persons were selected for training the model; representing the executive office user, personal assistant and the secretary (CEO, P. A & SEC.). 400 images were obtained from the face of each of them making a total of 1200 images with which the model was trained for face recognition. 80 images of each person were reserved for testing (240 test images) representing 20% of the total images. The training begins with labelling which is a process of saving and naming the pictures in different folders which the model can recognize. The next step was the training of model. The labelled image folders were imported into the model to train with before classification. The screenshot of the training is as shown in Figure 8.

```

11 # our images are located in the dataset folder
12 print("[INFO] start processing faces...")
13 imagePaths = list(paths.list_images("training"))
14
15 # initialize the list of known encodings and known names
16 knownEncodings = []
17 knownNames = []
18
19 # loop over the image paths
20 for (i, imagePath) in enumerate(imagePaths):
21     # extract the person name from the image path
22     print("[INFO] processing image {}/{}".format(i + 1,
23         len(imagePaths)))
24     name = imagePath.split(os.path.sep)[-2]
25
26 # load the input image and convert it from BGR (OpenCV ordering)
  
```

```

(venv) [D:\IT\Projects\DigitalTagesRBP faceRecogn & python3] train_model.py
[INFO] start processing faces...
[INFO] processing image 1/3288
[INFO] processing image 2/3288
[INFO] processing image 3/3288
[INFO] processing image 4/3288
[INFO] processing image 5/3288
[INFO] processing image 6/3288
[INFO] processing image 7/3288
[INFO] processing image 8/3288
[INFO] processing image 9/3288
[INFO] processing image 10/3288
[INFO] processing image 11/3288
[INFO] processing image 12/3288
  
```

Fig.9. Screenshot of training of model

The performance of the trained model was tested by importing the test images into the FaceNet thus generating embedding which are distinct feature vectors which represent the characteristics of the faces. Recognition was then done by comparing the similarities based on the Euclidean distance (shown in equation (5)) between the embeddings [10-14].

$$d = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2} \quad (5)$$

where,

(x_1, y_1) = coordinates of one point.

(x_2, y_2) = coordinates of the other point.

d is the distance between the coordinates of the two points

A threshold was then set that determines whether the face embeddings are considered a match or not.

3.6. Mode of Operation

The system was designed and installed with capabilities for decision making. It is able to know when some services like lightings, air conditioner should be put on or off. It was designed to recognize who is authorized to enter the office. The door which is equipped with an ultrasonic sensor senses the presence of a person then activates the camera. The camera scans the image, sends to the processor where it is compared with the image of the stored face; the image with which the model was trained. If the faces match, the door opens and the room light switched on, the door closes after 10 seconds, air conditioner and the television / To Do screen (to remind him of the scheduled work for the day) are switched on after 5 minutes. They remain ON even if he leaves the seat for 30 minutes after which they automatically go off. Likewise, the light bulb remains on for 30 minutes after he has left the office. The office user can generate a one-time pin (OTP) that a person he sends to take or do something in the office can use for access. Most of the fire accident that occur in offices are electrical in nature, therefore this system has the ability to send sms alert when high current/voltage is detected and simultaneously switch off the office electrical network.



Fig.10. The complete system housed in a transparent chassis

Table 2. Accuracy of image recognition

S/N	DATA CLASSES	ACURRACY (%)
1	CEO	86.40
	SEC	86.01
	P. A	86.10
2	CEO	87.00
	SEC	86.67
	P. A	86.82
3	CEO	87.50
	SEC	87.21
	P. A	87.00
4	CEO	88.01
	SEC	87.85
	P. A	87.88
5	CEO	88.64
	SEC	88.17
	P. A	88.27
6	CEO	89.43
	SEC	89.02
	P. A	89.10
7	CEO	90.37
	SEC	89.75
	P. A	90.00
8	CEO	91.40
	SEC	90.89
	P. A	91.03
9	CEO	92.31
	SEC	91.81
	P. A	91.99
10	CEO	93.13
	SEC	92.98
	P. A	93.01

4. Finding and Analysis

This section presents the results obtained in the study and the findings which were extensively discussed. The whole assemblage housed in a room-like transparent chassis is as shown in Figure 10. The shape of the chassis

was thus made to mimic a building with door for access control, while its transparency helps to view the components, circuit board and the appliances inside the office as they operate.

4.1. Image Recognition

The image recognition model was tested with 40 images from each data class, representing 20% of the dataset. The accuracy was determined using the Euclidean distance according to equation 5. This is based on the distance or similarities between training and testing images. The results were obtained and the summary is as tabulated in Table 2. The least accuracy was 86.01% while the highest was 93.13%, which means that the similarities between the input images and output of the model were very high.

4.2. Results of Test on the Electric Power Monitoring Module

The electric power monitoring unit was tested for its ability to sense the supplied voltage level. A high precision SUNTEK-3000 variac that smoothly adjust the AC voltage in the range of 0-300v ac was used for the testing and the parameters obtained tabulated in table 3. From 1v ac to 160v ac which represented low voltage supply, the office electrical network was switched OFF while a SMS message (“IRREGULAR SUPPLY: Power shut down”) was sent to the mobile phone of the administrator. At 161v ac which represented the useable voltage level, the electrical network was switched ON and a SMS message (“NORMAL SUPPLY: Power restored”), the status remains the same until the supply exceeded 220v ac. From 221v ac to 300v ac which represented high voltage, the office electrical network was again shut down and SMS message of irregular supply sent to the admin phone.

Table 3. Results of test of the power monitoring module

S/N	Voltage Range	Power Status	SMS Alert
1	1 – 20	OFF	IRREGULAR SUPPLY: Power shut down
2	21 – 40	OFF	Nil
3	41 – 60	OFF	Nil
4	61 – 80	OFF	Nil
5	81 – 100	OFF	Nil
6	101 – 120	OFF	Nil
7	121 – 140	OFF	Nil
8	141 – 160	OFF	Nil
9	161 – 180	ON	NORMAL SUPPLY: Power restored
10	181 – 200	ON	Nil
11	201 – 220	ON	Nil
12	221 – 240	OFF	IRREGULAR SUPPLY: Power shut down
13	241 – 260	OFF	Nil
14	261 – 280	OFF	Nil
15	281 – 300	OFF	Nil

Table 4. Some existing design of smart systems as compared with the current study

S/N	Author(s) Year of Publication	Means of Transmission	Area Covered
1	Alsaad & Hussien (2021)	GSM	Access control
2	Anwar & Kishore (2016)	Email	Access control
3	Toubidul <i>et. al.</i> (2023)	GSM	Access control
4	Olaniyan <i>et. al.</i> (2020)	GSM	Appliances control
5	Noora & Baswaraj (2019)	Email	Appliances control
6	Current Study (DEVELOPMENT OF A FACENET ENHANCED SECURED SMART OFFICE SYSTEM)	GSM	Access Control, Appliance Control/ Management and Prevention of fire outbreak

5. Conclusions

FaceNet enhanced secured smart office system has taken office automation to a new level. The deep learning model used Euclidean distance for image recognition, this has helped to produce a high precision users’ authentication system which unlike earlier designs is completely autonomous. The power monitoring module completely isolated the

office from irregular power supply which prevents the possibility of electrical fire outbreak. The combine features of access control, electrical fire prevention and smart switching of appliances made this study stand out for combining all the goals of automation in a simple system. This research also shows that secured and smart office automation system can be achieved cheaply from low-cost locally available components and used to control a variety of office appliances ranging from light bulbs, televisions, air conditioner and the entire office electrical system. The essential components are so small and few that they may be put in a little inconspicuous container. The developed smart office system was tested and certified to granting access to authorized persons only and managed various devices such as lighting system, air conditioning system, Television and computer systems, and many others. As a result, this system is scalable and adaptable.

6. Future Scope

To further strengthen the security of the smart office in the future, it could be equipped with devices to recognize intrusion attempt, capture the image of the intruder and transmit to the administrator. The office can also be made smarter by including a deep learning based advisor or reminder.

Reference

- [1] Divyashree D A, Dr. B R Sujatha, Energy Management System for Office/Home Automation, *International Journal of Engineering Research & Technology (IJERT) NCETESFT – 2020*, Vol. 8, Issue 14, 2020.
- [2] Adelakun, N. O. & Omolola, S. A., Development and Testing of Arduino Timer Socket, *WSEAS Transactions on Advances in Engineering Education*, Vol. 20, Pp. 7-13, 2023, <https://doi.org/10.37394/232010.2023.20.212-20>
- [3] Olajide M. B., Adelakun, N. O., Kuponiyi, D. S., Jagun, Z. O. & Odeyemi, C. S., Design of An Automatic License Plate Reader, *ITEGAM Journal of Engineering and Technology for Industrial Applications, Manaus*, v.8 n.37, 21-27, 2022. <https://doi.org/10.5935/jetia.v8i37.833>
- [4] Folorunso C. O, Raheem W. A, Okutubo A, Ayininuola O., Voice-Activated Small Office Automation and Security System using Raspberry Pi. *ABUAD Journal of Engineering Research and Development (AJERD)*, Vol. 4, Issue 2, 36-42, 2021.
- [5] Wai, L., Malik, N. & Bodwade, Y., Literature Review on Home Automation System Literature Review on Home Automation System, *Int. J. Adv. Res. Comput. Commun. Eng. ISO*, 6(3), 733-737, 2017.
- [6] Bo J., Leandro C. and Nuno C., Deep facial diagnosis: deep transfer learning from facial recognition to facial diagnosis. *IEEE Access*, 8 (2) 123649-123661, 2020.
- [7] Anwar S. and Kishore D., IoT Based Smart Home Security System with Alert and Door Control using Smart Phone. *International Journal of Engineering Research & Technology (IJERT)*, 5 (12) 504-509, 2016.
- [8] Tuzcuoğlu, D., de Vries, B., Yang, D. and Sungur, A., "What is a smart office environment? An exploratory study from a user perspective", *Journal of Corporate Real Estate*, Vol. 25 No. 2, pp. 118-138, 2023. <https://doi.org/10.1108/JCRE-12-2021-0041>
- [9] Gomathy, C. K., Keerthi, K., and Pavithra N., Smart door with facial recognition. *International research journal of engineering and technology*, volume 08 (10), 471-474, 2021.
- [10] Bhuyar Renuka and Ansari Saniya, Design and Implementation of Smart Office Automation System. *International Journal of Computer Applications (0975 – 8887)* 151 (3) 37-46, 2016.
- [11] Shaikh S. A. and Kapare A. S., Smart Office Area Monitoring and Control Based on IoT, *International Journal of Engineering Research in Computer Science and Engineering*. Vol.4, Issue 4, 48-52, 2017.
- [12] Prasetyo T. F., Zaliluddin D. and Iqbal M., Prototype of Smart office System Using IoT based Security System. *4th international Seminar of Mathematics, Science and Computer Science Education IOP Publishing Conference Series: Journal of Physics*, 2018. doi :10.1088/1742-6596/1013/012189
- [13] Prentice C. T. and Karakonstantis G., A Smart Office System with Face Detection at the Edge. *IEEE Smart World Congress: Proceedings 2018 ed.*, pp. 88-93, 2018.
- [14] Apurva Shashank and Rajiv Vincent, An Innovative Approach for Secured Smart Office and Home System using IoT, *Journal of Physics, National Science, Engineering and Technology. IOP Publishing*, 1716 012056, 2021. <https://doi.org/10.1088/1742-6596/1716/1/012056>
- [15] Arun S., Anjaneya R., Dharshan K. and Srinivasa N., Smart Office Monitoring System Using IoT, *International Research journal of Engineering and Technology*, 06 (4) 4560-4564, 2019.
- [16] Adelakun, N. O., Olanipekun, B. A. & Omolola, S. A., Design and Testing of a Hybrid Distribution Board, *ITEGAM Journal of Engineering and Technology for Industrial Applications, Manaus*, v.7 n.32, Pp. 39-43. Nov/Dec, 2021. <https://doi.org/10.5935/jetia.v7i32.788>
- [17] Abubakar I. N, Ufort E. G, Dodo U. A, Okosun O. E, Dodo M. A and Babalola O., Internet of Things (IoT) Based Office Automation System. *Zaria Journal of Electrical Technology, Department of Electrical Engineering, Ahmadu Bello University, Zaria Nigeria*. Vol. 10, issue 1, 12-18, 2021.
- [18] Jagruti, K, Mishra, E., A Sandeep, K. Mishra, S. Priyanka, "Home Automation Using Wi-Fi Interconnection", *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, Vol. 6, No. 8, pp 6-9, 2019.
- [19] Alsaad S. N. and Hussien N. M., IoT based message alert system for emergency situations, *International Journal of Computing and Digital Systems*, 10 (1) 1123-1130, 2021.
- [20] Adejumobi O. K., Sadiq M. O., Ayeni M. O., Fawole A. O. and Fakunle A. O., Development and Implementation of a PC-based Home Automation System using USB Protocol. *International Journal of Engineering and Technology research*, Published by Cambridge Research and Publications, 18 (5) 153-162, 2020.

Authors' Profiles



Charity Segun ODEYEMI, a lecturer in Computer Engineering Department at The Federal University of Technology, Akure Nigeria has more than six years of research and academic experience. He holds Bachelor, Masters in Computer Engineering and a PhD in Energy and Solid States. He has been involved in several researches in Computer Engineering, Electronics, Energy and Smart systems with several publications.



Olatayo Moses OLANIYAN is an Associate Professor of Computer Engineering at Federal University, Oye Ekiti Nigeria. Having more than fifteen years' experience in academics, he has graduated several Masters and PhD students, he is an authority in AI and embedded systems. He has more than 60 publications which include books, journals and proceedings.

How to cite this paper: Odeyemi C. S., Olaniyan O. M., "Development of a Facenet Enhanced Secured Smart Office System", International Journal of Intelligent Systems and Applications(IJISA), Vol.16, No.1, pp.41-51, 2024. DOI:10.5815/ijisa.2024.01.04