Automated door with face recognition: using artificial neural network approach

A Bashir1, N M Tahir1, A Y Zimit2, U I Bature3,4, K A Abubakar5 and A Y Nasir3

1Department of Mechatronics and System Engineering Abubakar Tafawa Balewa University Bauchi, Nigeria
2University of Hafr Albatin, 39524 Hafar Al Batin City, Saudi Arabia.
3Department of Computer and Communications Engineering, Abubakar Tafawa Balewa University Bauchi, Nigeria.
4Department of Electrical and Electronic Engineering, Universiti Teknologi Petronas, Malaysia.
5Department of Materials & Metallurgical Engineering, Nigerian Army University Biu, Borno, Nigeria.

nuratahir85@gmail.com, biusman@atbu.edu.ng

Abstract. The implementation of an accurate face recognition system in a hardware device is a very important aspect of various security applications. In a security system, any type of password is used to access private and confidential data, some are hard to remember and can be stolen or guessed, misplaced, forgotten, purloined or duplicated, or become corrupted and unreadable. While there have been significant improvements in the algorithms with increasing recognition accuracy, only a few types of research were conducted on implementing these face recognitions in hardware devices. Door access control systems based on face recognition is geared towards simplifying much-difficult face recognition problems in uncontrolled environments. This report comprised mainly of three sub-phases: face detection, face recognition, and automatic door access control. The face is detected by using the Viola-Jones method and face recognition is implemented by using the Principal Component Analysis (PCA). If a face is recognized, it is known, else it is unknown. The door will open automatically for the known person due to the command of the microcontroller (Atmega328P) received from the MATLAB program. On the other hand, the alarm will ring for an unknown person.

1. Introduction

Security is an aspect that is given top priority by organizations, educational institutions, political and government in personal identity and forgery issues [1], also the demand for going smart is continuously increasing [2]. Although the risk and security issues concern related to this category of systems may be enormous, the inclusion of a more general model of privacy and security in the design phase will reduce a lot of risks that are classified as moderate [3]. Monitoring door entrance is a vital issue, considering it as the only means of structure access. So, an efficient and precise door security system is vital to secure our assets and properties. Nowadays, manual or traditional methods of things are evolving to smart access control. Therefore, there is a need to change our traditional methods of accessing things to modernize methods of smart connectivity, this will provide enhance security and eliminate the existing drawbacks. Security separate access and threats, access control constitute three main components; identification, authentication, and authorization, thus there is a need to actualize this component on door system for better security and control [4-6]. Traditional door access requires keys, and existing ones requires a password using the keypad, pattern, card, or identification ID [7].
Interestingly, human face image has analogous features to fingerprint, they have uniqueness and they are nonexchangeable. Therefore, face image remains the potential means for substituting password, card, and PIN-based security systems [7]. Drawbacks in password, PIN, and card security systems are easily transferable, guess, or crack. Password or PIN are commonly created using names, special dates of the user or user’s family, etc. Furthermore, keys can be misplaced, the password is easily leaked through phones, handbooks, or jotters. They can be hard to remember, if stored in a memory device, the device may be corrupted thus rendered unreadable. The traditional lock using keys or password system and the use of radio frequency identification (RFID) lock systems requires keys, PIN, and cards respectively, these systems do not verify the authenticity of the user [8, 9]. Therefore, the security level of these systems seems to be diminutive. But a system that generates a one-time password (OTP) or uses a near field communication tends to be more secured [10]. However, obtaining the OTP requires extra communication linkage between the device and a server which often seems to be unreliable. Using the encryption method is another good technique of establishing security in locking systems [11], only the users who know the key can have access to the system since the original information is being transformed to another format [12]. However, the setbacks with this are losing the key which renders the system vulnerable, and security level depends upon the surety of the encryption keys, it can be too slow, and energy-consuming and complex system [13]. The IoT based security lock system interacts with the server to provide some level of security [14], but the user normally transmits his confidential information over the network, such may offer his confidential data vulnerable to attackers. Thus, by developing a face recognition system, it will be more secure because the facial image had to be used as the ID. It will also help in avoiding any duplicated identification. Either for security or human-computer interaction, there is a wide application to face recognition. Recent developments in communication technology and the call for better security applications have turned face-recognition into focus. Face recognition systems have become the subject of increased interest [15]. Chances of unauthorized access to critical information and infrastructure have become a major concern [16]. Thus, a system must be implemented so that the security system becomes more robust and the probability of unauthorized access to the system becomes minimal.

The general idea of face recognition is to extract certain data from the region of interest of a human facial image and to compare them to stored data for identification. Face identification identifies an input image that belongs to a person in a database whereas face verification searches for the existence of a person’s image in the database. The feature extraction stage represents the backbone of face recognition systems because of the direct dependency on the accuracy of the extracted facial features. In this system, Viola jones method of face detection is used, since it has been developed with a scale of the invariant detector [17]. Principal Component Analysis (PCA) is an effective face recognition method, it involves feature extraction, reduction, and classification [18]. Face recognition is realized using the PCA algorithm, and the Euclidean method of classification and recognition is used. This system is implemented using a microcontroller (Atmega 328P), it possesses good features and integrated peripherals, the microcontroller is used to receive the signal sent from the personal computer (PC) that process the software programming of the face recognition system that was developed using MATLAB© and send a command back either to the door motor circuit or to the alarm circuit. The connection between the microcontroller and the PC is achieved using USB (RS232) converter, facial image databases are used to study the behaviour of the proposed face recognition system under various types of images. There are two cases in this system. The first is an automatic door opening for the recognized person (known) and the second is ringing the alarm for the unauthenticated person (unknown). This proposed smart door automation system using the face recognition method, since it has become an important research area because of its usefulness in numerous applications such as access control, security systems, credit card verification, and criminal identification.

2. Research method
Artificial Neural Network (ANN) is an information processing model just like the biological nervous systems of the brain processes information.
In simpler terms, ANN is a mathematical model of the brain which is used to process nonlinear relationships between inputs and outputs data or information. In this work, the supervised learning of ANN is used with the K-nearest neighbour algorithm of the lazy learner’s method to store all the instances that correspond to the training data in n-dimensional space. This algorithm is used because it does not focus on constructing a general internal model. Instead, it works on storing instances of training data. The overall block diagram of automatic door-access system using face recognition is shown in figure 1.

**Figure 1.** Overall block diagram of automatic door access system using face recognition

2.1. **Arduino Uno/Microcontroller (ATMEGA 328P)**

The selection of the appropriate hardware device for the proposed door access control system is important to achieve higher recognition accuracy and high performance. In this paper, the Arduino hardware platform is used due to its good features and integrated peripherals as shown in figure 2. The microcontroller is used to receive the signal sent from the PC and send a command back either to the door motor circuit or to the alarm circuit.

**Figure 2.** Arduino Uno Board

The ATmega328 chip found on the Uno has the following specifications:

- Flash 32k bytes (of which 5k is used for the boot loader)
- SRAM 2k bytes
- EEPROM 1k byte

2.2. **Motor Driver (L293D)**
The Device is a monolithic integrated high voltage, high current four channel driver designed to accept standard DTL or TTL logic levels and drive inductive loads (such as relays, solenoids, DC and stepping motors) and switching power transistors. A separate supply input is provided for the logic, allowing the operation of the DC motor to move backwards and forward. The flowchart for the automatic door closing and opening system is shown in figure 3.

**Figure 3.** Flowchart for the automatic door opening and closing system

2.3. **DC Motor**

A motor converts electrical energy into mechanical energy. There are two types of motor: AC motor & DC motor. A simple DC motor uses electricity and magnetic field for producing torque which rotate the motor. The applied voltage describes the speed of motor while current in the armature windings shows the torque. If applied load increased in the motor shaft, then in order to sustain its speed, the motor draws more current from the supply. If the supply is unable to provide enough current, the motor speed will be affected. In this research, the motor is used to drive the door to and fro to give access into or out of the building.

2.4. **Buzzer**
A buzzer is a small yet efficient component to add sound features to the system. It is a very small and compact 2-pin structure. Hence it can be easily used on breadboard, perforated board and even on PCBs, this makes it a widely used component in most electronic devices. This buzzer can be powered using a DC power supply ranging from 4V to 9V. A simple 9V battery can also be used, but it is recommended to use a regulated +5V or +6V DC supply. The buzzer is normally associated with a switching circuit to either turn it ON or OFF at the required time and interval. In this research work, the buzzer is used as an Alarm Circuit, where the user is to be notified about an intruder trying to access the door.

2.5. Push Button
A push-button (also known as button) is a simple switch mechanism for controlling some aspect of a machine or a process. The surface is usually flat or shaped to accommodate the human finger or hand, so as to be easily pressed or pushed. Buttons are most often biased switches, although many un-biased buttons (due to their physical nature) still require a spring to return to their un-pushed state. In this research, the push button is placed inside the room for the authorized person to press, thereby giving him/her access to go out of the room since high level of security inside the room is not needed.

2.6. Circuit Diagram of the Proposed System
The hardware configuration of this system is composed of the microcontroller (ATMEGA 328P), L293D driver IC, USB to RS232 converter, push-button, DC motor, and buzzer. USB to RS232 converter is used as the interface between the personal computer and the microcontroller. The push-button is used as the inputs of the microcontroller and other components are used as outputs of the microcontroller. This system used ATMEGA 328P microcontroller because of its good features and integrated peripherals. The microcontroller is used to receive the signal sent from the PC and send a command back either to the door motor circuit or to the alarm circuit. The simulation diagram of the proposed system using proteus software is shown in figure 4 while the hardware circuit of the proposed system is shown in figure 5.

**Figure 4.** Simulation Diagram of the Proposed System in Proteus

**Figure 5.** Hardware circuit of the proposed system
3. Results and analysis

3.1. Facial Database
In this work, facial image databases are used to study the behaviour of the proposed face recognition system under various types of images. There is a total of six images of three people; each person has two images with different poses and expressions. Only one image from each person is used for training and the remaining one image is used for the testing phase. This database is chosen because of the availability and simplicity of various instances of front views for each subject. Figure 6 depicts the facial databases of the proposed system.

![Facial databases of the system](image)

**Figure 6.** Facial databases of the system

3.2. Hardware simulation results
The overall automatic door access system using face recognition is simulated by using MATLAB. A MATLAB code is created to perform automatic face detection and recognition. There are two cases in this system. The first is an automatic door opening for the recognized person and the second is ringing the alarm for the unauthenticated person.

3.2.1. CASE I. When the test image is recognized as the authenticated person, the green LED will turn ON and the door motor is rotated with the reverse direction until the micro-switch one is activated. When micro-switch one is activated, the door motor is stopped. After five seconds, the red LED will turn ON while that of the green will go OFF and the door motor is rotated with forwarding direction until micro-switch two is activated. Figure 7 and 8 show the simulation results for the authenticated person.

![Simulation result](image)

**Figure 7.** Result when test face is detected and recognized as an authenticated person
3.2.2. **CASE II.** When the test image is not recognized as the authenticated person, the red LED will turn ON blinking ten times, and the door motor will not rotate, thus ringing an alarm to the user that an unauthenticated person is about to enter the home. Figure 9 and 10 show the simulation results for the unauthenticated person.

![Figure 8](image)

**Figure 8.** Hardware test for an authenticated person when door open

![Figure 9](image)

**Figure 9.** Result when test face is recognized as an unauthenticated person

![Figure 9](image)

**Figure 9.** Hardware test for an unauthenticated person when the door does not open

4. **Conclusion**

In this paper, an automatic door access system using face recognition and detection is presented. The automatic face detection and recognition are done by the MATLAB® program on PC. The microcontroller is used to control the door access system depending on the incoming data sent from the personal computer (PC). The door is opened immediately after confirming that the person is
authenticated. After five seconds, the door is closed automatically. The majority of previous research was focused on improving the accuracy of the face recognition algorithm in light of some problems such as illumination, pose, and facial expression changes. However, only a few of these studies focused on implementing these face recognition techniques with an embedded system, such as a door access control system. The problem of high computational time and high power consumption are also faced by current door access control systems either supervised or not fully automatic. Therefore, more research should be conducted in an embedded system taking into consideration problems such as illumination, pose, and facial expression changes.

Acknowledgments
The authors wish to thank the Department of Mechatronics and System Engineering, Abubakar Tafawa Balewa University Bauchi for the provision of laboratory’s equipment.

References
[1] Nag A, Nikhilendra J N and Mrutyunjay K 2018 Int. Conf. on Con. in Technol. (Pune) vol 3 (Pune: India) 1
[2] Dutta J and Roy S 2017 Int. Conf. on Cloud Computing, Data Sci. & Eng.-Confluence. (Noida: India) pp 237-242
[3] Jacobsson A, Boldt M and Carlsson B 2016 Fut. Gen. Comp Sys. B 56 719
[4] Wijaya I G P S, Husodo A Y and Jatmika A H 2016 Proc. Int. Sem. On Intel. Technol. and its Appl. (Lombok: Indonesia) pp 151-156
[5] Simon O A, Bature U I, Jahun K I and Tahir N M 2020 Int. J. Infor. & Commun. Technol. 9 212-220
[6] Tshomo K, Tshering K, Gyeltshen D, Yeshi J and Muramatsu K 2019 Proc. Int. Conf. on Converg. in Technol. (Bombay: India) pp 1-5
[7] Divya R S and Mathew M 2017 Proc. Int. Conf. on Cir., Power and Comput. Technol. (Kollam: India) pp 1-3
[8] Tombeng M T and Laluyan H S 2017 Proc. Int. Conf. on Cyb. and IT Serv. Managt. (Denpasar) vol 5 (Indonesia: IEEE) pp 1-5
[9] Ahtsham M, Yan H Y and Ali U 2019 Proc. Int. Conf. on Networ. Sen. and Contrl. (Banff, AB: Canada: IEEE) pp 448-453
[10] Brown D R L 2017 (Certicom Corp,) U.S. Patent 9,734,322
[11] Chen H, Liu J and Yang C F 2016 Advanc. in Mech. Eng. 8 1-7
[12] James A and Sarikak T 2020 Stud. in Indian Plac. Nam. 40 pp 9-15
[13] Sadkhan S B and Salman A O 2018 Proc. Int. Conf. on Advanc. Of Sust. Eng. and its Appl. (Wasit: Iraq) pp 105-108
[14] Ha I 2015 Int. J. Sec. and its Appl. 9 45-54
[15] Tham K Y, Cheam T W, Wong H L and Fauzi M F A 2020 Comput. Sci. and Technol. vol 603 (Singapore: Springer) pp 227-236
[16] Petrakis E G, Antonopoulos F, Sotiriadis S and Bessis N 2020 J. Amb. Intell. And Huma. Comput. 11 929-943
[17] Tavallali P, Yazdi M and Khosravi M R 2017 Proc. Int. Conf. on Comput. Sci. and Comput. Intell. (Las Vegas: USA) pp 828-831
[18] Barnouti N H, Al-Dabbagh S S M, Matti W E and Naser M A S 2016 Int. J. Advan. Computer Sci. and Appl. 7 371-377