ICSAR

DESIGN OF A FINGER PRINT SCAN DOOR USING ARDUINO ATMEGA 328P AT KANO STATE POLYTECHNIC, NIGERIA

Mariya G. Mustapha [*], Auwal S. Yunusa [2], Auwal R. Dan Sharif [3], Auwal Usman[4], Umar Shehu[5], Nafisa Tijjani[6], Aliyu Sani Yahaya[7], Usman Haruna[8]

[2,5,6,7]*Department Mechatronic Engineering, Kano State Polytechnic, Nigeria*
[1,3,4,8]*Department Electrical Engineering, Kano State Polytechnic, Nigeria*

[*](*auwalsalis1984@gmail.com*) *Email of the corresponding author*

Abstract – This article includes a smart and affordable door lock enhanced with a fingerprint interface. For implementing this research, we will be using Arduino atmega328p, a fingerprint sensor, a motor driver, a motor, and other hardware devices. The fingerprint sensor will be integrated with the door panel, facing the outer side of the door, so that people can't have access to the controlling systems from outside. The latches will be fixed inside the door panel so that the thickness of the door can help the latch's strength. The fingerprint sensor will take the fingerprint of the user and forward it to the microcontroller to match its records. If the print matches with one of the fingerprints of the microcontroller's memory, the microcontroller will lock or unlock the latch, based on its current state. If the fingerprint is foreign to the microcontroller, the buzzer will buzz and the user will have to try again, if the wrong fingerprints are tried 5 times at most, the system will text the owner to alert him /her about a break-in. The system will also go into a secure state where it will continue to sound for alerting the neighbors that something is wrong. The system will reset once a known print is entered.

Keywords – Microcontroller, DC Motor, Fingerprint Sensor, Arduino, Buzzer

I. INTRODUCTION

The process of authenticating students sitting for examinations of various types continues to be a major challenge or an uneasy task for the invigilators in our institutions and is also time-consuming, as a result, other people often write examinations for other candidates. Hence, we chose to develop a system that doesn't need the interference of Human beings for Examination authentication. This system is designated to allow the passage of only users verified by their fingerprint scan and to block those whose scans are not recognized by the system. A formal examination can rightly be defined as the assessment of a person 's Performance, when confronted with a series of questions, problems, or tasks set for him/her, in order to ascertain the amount of knowledge that he has acquired, the extent to which the person is able to utilize it, or the quality and effectiveness of the skills he/she has developed.

During the 19th century, formal written examinations became regular in universities, schools, and other educational institutions. Examinations were also increasingly used for the selection of recruits to the civil service, and the professions, and to posts in industry and likewise. Over the ages, standardized testing has been the most common methodology, yet the validity and credibility of the system are still in question. This brings into focus the issue of examination malpractices. Malpractices can be defined as dereliction from professional duty, whether international, criminal, or merely negligent, by one rendering such professional services, that result in injury, loss, or damage to the recipient of those services, or those entitled to rely upon them, or that

affect the public interest adversely Encyclopedia Britannica (1769). Examination malpractice in the Nigerian educational system is highly disturbing and manifests in a variety of forms, but our project is based on impersonation. This involves arrangements for someone other than a candidate, usually for a fee or some other considerations.

Two types of systems that help automatically establish the identity of a person are: Authentication (verification) system. Authentication is the process of determining whether someone is in fact, who or what he/she declares himself to be. Authentication technology provides access control for systems by checking to see if a user's credentials match the credentials stored in a database of authorized users. This project topic is based on this type of identity system. Identification systems. Identity refers to the condition of being a specified person, or the condition of being oneself and not another. The process of recognizing that specified person is known as identification. In a verification system, a person who desired to be identified submits an identity claim to the system; these include:
- Appearance
- Names
- Knowledge
- Bio-dynamics
- Passwords
- Personal identification number(PIN)
- Stripe cards/smart cards

These are no longer considered reliable enough to satisfy the security requirements of electronic transactions or differentiate between an authorized person and an impostor as in the case of examinations, who fraudulently acquires the access privilege of the authorized person. The topic of this project is channelled towards the development of an examination impersonation elimination system and this system would strictly do with the unique feature of identification by means of a fingerprint.

A. LITERATURE REVIEW

Rana and Sachin (2016), presented a paper titled "Vehicle Ignition using Fingerprint Sensor". The proposed system includes Fingerprint Sensor, Liquid Crystal Display, microcontroller, and GSM module. Rather than using the key of the car to start the vehicle, the fingerprint is used to ignite the vehicle. The Fingerprint sensors take in the fingerprint of the user which in turn sends the signals to the microcontroller which then matches the scanned fingerprint with the ones that are stored in its database. Once the fingerprint is matched, the microcontroller then sends the desired signal to the vehicle after which the user can start the vehicle. Whenever a non-authenticated person tries to scan his fingerprint, a message is sent to all the registered users via the GSM module. Gangi and Gollapudi (2013), implemented a locker security system that used fingerprint, password, and GSM technology for activating the locking system. The system authenticates and validates the user, then unlocks the door in real time for the locker secure access. Kaur (2010), designed a microcontroller-based home automation system that focused on home security. The home security comprised a password-based locking system, an automatic switching system, a temperature-controlled cooling system, a lighting system, and fire and smoke sensors. Olaniyi and Buhari (2018), in their paper, presented an approach that mainly involves capturing the fingerprint of different users which will be used as their password to gain access to a secured area. The false acceptance rate (FAR) and false rejection rate (FRR) performance metrics were used to evaluate the system performance and the result shows that the FAR yielded 10% compared to the FRR which gave 20%. The widespread adoption and implementation of the developed access control system will provide a platform to enhance personal safety and a high level of confidentiality in the door access control system.

In carrying out this research, we used the ATMega328 microcontroller, fingerprint sensor, liquid crystal display, and DC motor which drives the door when a student is authenticated, thereby reducing problems of impersonation during an examination in our great institution.

II. MATERIALS AND METHOD

The system consists of a fingerprint scanner connected to a microcontroller circuit. The person needs to first scan his finger on the scanner for enrolment to save the fingerprint in the system. For the authentication process, after placing your finger on the scanner, the microcontroller now checks the person's fingerprint validity. If the fingerprint is

authorized the microcontroller now sends a signal to two relays whose function is to operate a motor driver to open and close the door. This ensures that only authorized users are allowed to enter the examination section and unauthorized users are not allowed to enter.

Some of the problems which were encountered in the previous identification systems are:
- Student impersonation
- Insecure authentication of students
- Manual verification of student
- Corruption in Examination System

The design and construction of the fingerprint door security system have the following limitation: the fingerprint sensor is the only device that can scan and sense the fingerprint of the user so as to open the door and any fingerprint that does not match with the user's fingerprint it means the door will remain closed.
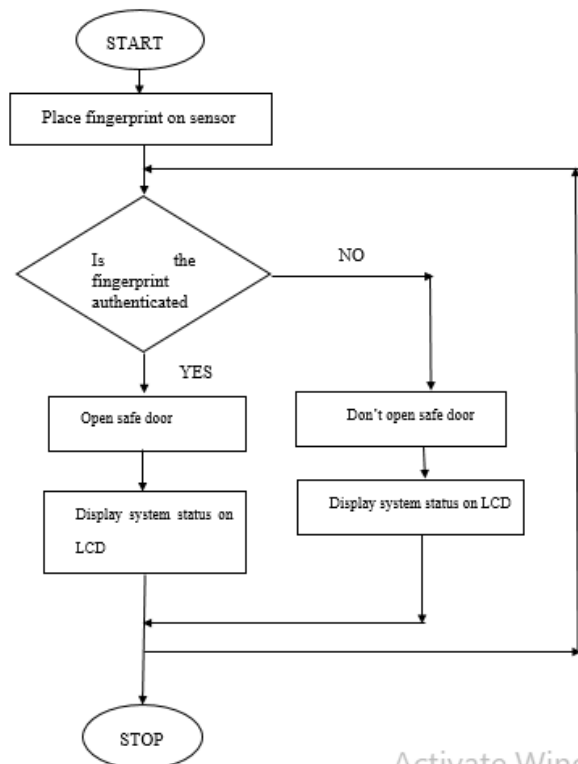

Fig 1. Flow Chart of the System

After switching on the circuit, the enrolment process is to be done, whereby Enrol button is pressed and a finger is asked to be placed on the fingerprint module, the finger is then removed, and then the system request the user to place the finger to be scanned for the second time, then it will be stored. During authentication, when a student places

his finger on the fingerprint scanner, the fingerprint obtained will be compared against the stored template that is already stored in its memory, if a match is found it shows an acknowledgment in its display and grant access to the door, if there is no match of the fingerprint, it displays finger not found and will not grant access.

III. RESULTS

A series of tests were carried out before and after the design of this research using a multimeter. These tests include testing components to see if they are functional. The circuit was tested for registered and unregistered fingerprints and it worked correctly. The results are shown in the figures below.

Fig. 2. First step of enrolment process

Fig. 3. Second step of enrolment process

Fig. 3. Third step of enrolment process

Fig. 4. Result for stored fingerprint

Fig. 5. Display for unregistered finger

Fig.6. Result of test for unregistered finger with door closed.

Fig.7. Result for authorized print and ID number

Fig. 8. Result of test for registered finger with door opened

IV. DISCUSSION

The aim of this research is to design a system which allows an examination hall door to open upon the scan of the verified students fingerprint and to disapprove for non-verified individual. Having realized the device and found it working properly according to its design specifications and coupled with the facts that relatively cheap components were involved in its realization, and also very easy to use, the aim of the project can be said to be achieved. The system can be used as an effective security system against impersonation in our tertiary institutions.

REFERENCES

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

[2] J. Breckling, Ed., *The Analysis of Directional Time Series: Applications to Wind Speed and Direction*, ser. Lecture Notes in Statistics. Berlin, Germany: Springer, 1989, vol. 61.

[3] S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, "A novel ultrathin elevated channel low-temperature Poly-Si TFT," *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

[4] M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[5] R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, "High-speed digital-to-RF converter," U.S. Patent 5 668 842, Sept. 16, 1997.

[6] (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[7] M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available: http://www.ctan.org/tex-archive/macros/latex/contrib/supported/IEEEtran/

[8] *FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

[9] "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[10] A. Karnik, "Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP," M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

[11] U. Ozkaya, Ş. Öztürk, K. Tuna, L. Seyfi and B. Akdemir "Faults Detection With Image Processing Methods In Textile Sector" In 1st International Symposium on Innovative Approaches in Scientific Studies (pp. 11-13), 2018.

[12] *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification*, IEEE Std. 802.11, 1997.