MPRI-JERT | INTERNATIONAL JOURNAL OF ENGINEERING & RESEARCH TECHNOLOGY
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

BIOMETRIC FINGER PRINT EXAMINATION AUTHENTICATION SYSTEM

G.N. JOLA[1] AND YUNUSA M.A[2]
[1&2] *Department of Electrical and Electronics Engineering Technology, Federal Polytechnic, Bauchi State, Nigeria.*

Abstract

Biometric Fingerprint based exam hall authentication systems assist in the elimination of examination impersonation. The Nigeria institution examination control board is yet to use the fingerprint as mode of identification, thus this has resulted in people sitting for examinations for others who collect the result at the end. With the adoption of fingerprint biometric, this will be eliminated as fingerprint identification will also be used during collection of results and certificates. This target can be mainly decomposed into image pre-processing feature match. Based on the analysis, an integrated solution for fingerprint recognition is developed for demonstration. This demonstration program is coded using visual Basics programming language for the program, some optimization at coding level and algorithm level are proposed to improve the performance of this fingerprint recognition system. These performances enhancements are shown by experiments conducted upon a variety of fingerprint images.

KEYWORDS:
Biometric, Examnation, Authentication, Finger, System.

Introduction

Authentication has always been a major challenge in all types of examination. Verification of the authentic candidate is not an easy task, and also it consumes a lot of time and process. 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 him/her, in order to ascertain the amount of knowledge that he has acquired, the extent to which he 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 employed for the selection of recruits to the civil service, and the professions, and to posts in industry and commence. Over the ages, standardized testing has been the most common methodology, yet the validity and credibility of the expanded range of contemporary assessment techniques have been called into question.

There are two types of systems that help automatically establish the identity of a person:

Authentication (verification) systems and Identification systems.

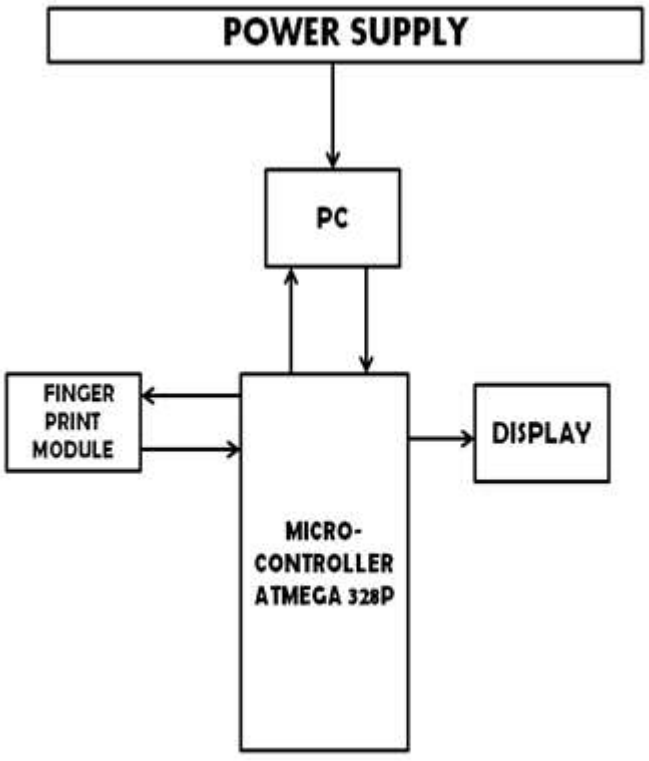

Figure 1: Block diagram

In a verification system, the identity claim of the individual is submitted to the system, usually via a magnetic stripe card, login name, smart card, etc. However, and the system either rejects or accepts the submitted claim of identity (Am I who I claimed to be?). In an identification system, the system establishes a subject‘s identity (or fails if the subject is not enrolled in the system database) without the subject‘s having to claim an identity (Who am I?). This research work is channeled

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

towards the development of examination impersonation elimination system and this system would strictly do with the unique feature of identification by means of finger print. A verification system based on fingerprints, and the terms verification, authentication, and identification are used in a loose sense and synonymously. Accurate automatic personal identification is becoming more and more important to the operation of our increasingly electronically interconnected information society. Traditional automatic personal identification technologies to verify the identity of a person, such as a personal identification number (PIN), or as an identification (ID) card, key, etc., are no longer considered reliable enough to satisfy the security requirements of electronic transactions or differentiate between an authorized person and an impostor who fraudulently acquires the access privilege of the authorized person. Biometrics is a technology that uniquely identifies a person based on his physiological or behavioral characteristics. It relies on —something that you are to make personal identification and therefore can inherently differentiate between an authorized person and a fraudulent imposter. Exams malpractice is an academic dishonesty or academic fraud. In fact both of these notions can be used interchangeably. Malpractices do not only refer to student, but to staff too. There are a lot of different types of examination malpractice, but most general ones are:

1. Plagiarism reproduction of someone works without any sort of attribution or reference to original author.
2. Fabrication: falsification of data information, or reference source.
3. Lying: giving wrong info to educational staff.
4. Cheating: an attempt to take in helpful material for the exam but in a way that the instructor or examiner does known about.
5. Bribery: getting the right answers or marks for money.
6. Sabotage: an attempt to prevent others from passing the exams, this include among other things, tearing pages from their books, deliberate damage to someone else work

An examination board is an organization that sets examinations and is responsible for marking them and distributing results. Examination boards have the power to award qualification to students. Most exam boards are running as non-profit organizations. the higher institutions in, which can offer qualification in variety of discipline and well-structured certificates, such as High certificates, Diplomas, Honors Degrees, Master degrees and Doctorates in different Disciplines to be recognized higher institutions such as the universities, polytechnic respected

colleges of education etc which need to establish a secure methods of registration, verification, identification and authentication to make sure that those who registered at the beginning of the year are the ones will who seat for the exam The systems that are used currently in the higher institutions are not secure because it requires a student to provide certain physical documents such as student cards, examination admission slip; etc. This types of methods (documents) can be forged by almost anyone in this fast growing computer technology world. Hence the need for the Adoption of Fingerprint Based Exam Hall Authentication system that permit only registered student to enter exam hall and block anyone who wasn't registered.

Aim

The aim of this work is to build a fingerprint examination authentication system

Objectives

1. Development of a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter.
2. Development of a level converter (like MAX232) is required for interfacing with PC serial port.
3. Development of an Optical biometric fingerprint reader

Scope

This work is to reduce if not eliminate malpractice in examination centers completely because there is a security alarm system incorporated, which alert securities around for any person coming in for impersonation and will be punish according to the examination rules. Also it can be use to give permission or access to students sitting for the examination, without the display of the students already uploaded data/information into the data base of the examination body, the students will not be granted entrance into the hall.

LITERATURE REVIEW

Introduction

A number of works has been done by several authors in the area of biometric technology and mobile communications over the years to the problem of entity entry/exit control. In Abdul Kadir et al (2009) proposed an RFID matrix card based

auto identity system to the manual problem of monitoring student in boarding schools. Upon initial study of the three Boarding school in Malaysia, current process of maintaining students records in and out was not only tedious, misinformation always happen as students tend to provide inaccurate information.

In Matjaz and Tusar (2007), a flexible modular system based on integration of arbitrary access sensors and an arbitrary number of stand-alone modules were applied to solve the problem of entity exit/entry. The system was tested with four sensors: a door sensor, an identity card reader, a fingerprint reader and a camera. However, identity cards can be lost, stolen and misused. Bochkov N.P et al (2007) examined the security problem of identity theft where he specifically addressed the following issue: Why should we care about identity theft? What options are available to solve this problem? What the solutions are? And why some are more effective than others? Vijay and Dattatray (2010) discussed the issue of using multimodal biometrics in systems. Biometric systems based on single source of information are called unmoral system. Publicized biometrics because of their uniqueness and consistency over time, fingerprints have been used for identification for over a century, more recently becoming automated (i.e. a biometric) due to advancements in computing capabilities. It became popular as a means of identification and verification because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use. N.P According to Miltonic et al. (2003), fingerprint is one of the most mature biometric traits and considered legitimate proof of evidence in courts of law all over worldwide. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering using fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology. The discovery of uniqueness of fingerprints caused an immediate decline in the prevalent use of anthropometric methods of identification and led to the adoption of fingerprints as a more efficient method of identification (Lee et al., 1991). With recent advances in internet and mobile technology, electronic service is becoming an important factor because different people can provide and obtain services without the limitation of location. The excellent e-service provides service via different channels and uses internet technology to provide customers with service in a cost

effective manner. Customer communities are managed through e-mail, SMS messages, faxes etc. (Hua et al 2004).

Finger Print Module:

This is a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. Which can store the finger print data in the module and can be configured in 1:1 or 1: N mode for identifying the person? The FP module can directly interface with 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port.

Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the homage of the fingerprint. A scratched or dirty touch surface can cause a bad image of the fingerprint. A disadvantage of this type of sensor is the fact that the imaging capabilities are affected by the quality of skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it is possible for an individual to erode the outer layer of skin on the fingertips to the point where the fingerprint is no longer visible. It can also be easily fooled by an image of a fingerprint if not coupled with a "live finger" detector. However, unlike capacitive sensors, this sensor technology is not susceptible to electrostatic discharge damage.

Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks spoor layer to an array Features

1. Integrated image collecting and algorithm chip together, All-in-one.
2. Fingerprint reader can conduct secondary development; can be embedded into a variety of end products.
3. Low power consumption, low cost, small size, excellent performance.
4. Professional optical technology, precise module manufacturing techniques.
5. Good image processing capabilities can successfully capture image up to resolution 500 dpi.

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

Of solid state pixels (a charge-coupled device).

Figure 1: UareU Fingerprint scanner

Microcontroller (ATmega328)

The Atmel 8-bit AVR RISC-based microcontroller combines 32 kilo byte (KB) ISP flash memory with read-while-write capabilities, 1 kilo byte KB electrical erasable programmable read only memory (EEPROM), 2 KB static random access memory (SRAM), 23 general purpose I/O lines, 32 general purpose working registers, three flexible timer/counters with compare modes, internal and external interrupts, serial programmable USART, a byte-oriented 2-wire serial interface, SPI serial port, 6-`channel 10-bit A/D converter (8-channels in TQFP and QFN/MLF packages), programmable watchdog timer with internal oscillator, and five software selectable power saving modes. The device operates between 1.8-5.5 volts. The device achieves throughputs approaching 1 MIPS per MHz

DESIGN AND CONSTRUCTION

Methodology

The proposed Biometric Examination authentication system uses fingerprint identification. In identification, the system recognizes individual by comparing his/her biometrics with every record in the database. In general, biometric identification consists of two stages:

i. Enrolment
ii. Authentication

During enrolment, the fingerprint of the user is captured (using a fingerprint reader, which are likely to be an optical scanner device, solid state or an ultrasound sensor or other suitable device) and the unique features are extracted and stored in database as a template for the subject along with the student ID. The objective of the enrolment module is to admit a student using his/her ID and fingerprints into a database after feature extraction.

These features form a template that is used to determine the identity of the student, formulating the process of authentication. The enrolment process is carried out by an administrator. During authentication, the fingerprint of the user is captured again and the extracted features are compared with the stored features in the database to determine a match. Features extraction performs some transformation of original features to generate other features that are more significant (Samina, *et al* 2014). The identification accuracy of a biometric system is measured with the false (impostor) acceptance rate (FAR) and the false (genuine individual) reject rate (FRR).

Biometric Finger Print Process

A fingerprint can be defined as an impression made by human finger because of the patterns created on the skin of our palms and fingers ever since birth. The marks or pattern on our finger will never undergo any change rather it becomes prominent with age. Figure 2 below shows a fingerprint image. For their permanence and unique nature, they have been used since long in criminal and forensic cases.

This fingerprint authentication system however, is cost-effective and simplified means of identification. The finger-print is distinctive to each individual. Even identical twins do not share the same fingerprint features, and it cannot be transferred, lost or forgotten like the password. It allows students to register for lectures with ease and eliminate errors that are associated with attendance registers because the system generates exports at the end of the semester. The advantage of this system is that it can work as a standalone system unlike other fingerprints identification systems already in existence. Forensic cases shown below, is a fingerprint pattern obtained from an optical sensor. The figure shows faint and dark lines emerging from a particular point and spiraling around it all over the finger

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

Figure 2: *A fingerprint image acquired by an optical sensor*

Enrolment

The enrolment process is done once for each person. Each person would be required to register their fingerprint pattern by record to know the attendance of a person or to know the number of times absent.

Verification Process

The second process is the verification process. This is the most repeated process. It is a done each time the user wants to make use of the fingerprint controlled device. When he places his finger on the fingerprint scanner surface, the fingerprint would be processed by the fingerprint scanner. The finger-print pattern that has been obtained would be compared against the stored enrolment template that is already stored in the database or memory location where the enrolment process was executed. When the fingerprint pattern passes the com-parson process, it shows an acknowledgement in its display and grants the user access.

Data Collection Process

The last process that will be done is the data collection process. The data about the fingerprint device usage or record can be collected after a period of time and can be used as a form of

Microcontroller ATmega328p Description (Design and Description)

The Atmel AVR core combines a rich instruction set with 32 general purpose working registers. All the 32 registers are directly connected to the Arithmetic Logic Unit (ALU), allowing two independent registers to be accessed in a single instruction executed in one clock cycle. The resulting architecture is more code efficient while achieving throughputs up to ten times faster than conventional CISC microcontrollers.

The ATmega328/P provides the following features: 32Kbytes of In-System Programmable Flash with Read-While-Write capabilities, 1Kbytes EEPROM, 2Kbytes SRAM, 23 general purpose I/O lines, 32 general purpose working registers, Real Time Counter (RTC), three flexible Timer/Counters with compare modes and PWM, 1 serial programmable USARTs , 1 byte-oriented 2-wire Serial Interface (I2C), a 6- channel 10-bit ADC (8 channels in TQFP and QFN/MLF packages) , a programmable Watchdog Timer with internal Oscillator, an SPI serial port, and six software selectable power saving modes. The Idle mode stops the CPU while allowing the SRAM; Timer/Counters, SPI port, and interrupt system to continue functioning.

Software Design

Fingerprint identification is based on two factors:

(i) Persistence: the basic characteristics and features do not change with the time,

(ii) Individuality: fingerprint of every person in this world is unique

To store the data of student present in the Attendance machine we have to build software which can store the data and schedule the data as per the student record. The data is feed to the software with the help of cable MAX 232. By the help of software the staff member can enroll the student class-test marks, attendance updates, as per student record.

Hardware Specification:

1. Microcontroller (At mega 328), it is used to store the database collected from student.
2. Hard Disk: 40 GB
3. Processor: Any processor above 500 MHz
4. RAM: Above 512 MB
5. Input device: Standard Keyboard and Mouse.
6. Output device: VGA and High Resolution Monitor.

Circuit Connections:

In this project, a fingerprint module is interfaced to a microcontroller with a serial interfacing, and this project uses a relay, a Buzzer, an LCD, and switches.
4-pin fingerprint scanners consist of VCC, RX, TX and Ground pins and are connected to 10, 11, 16 pins of the microcontroller, as shown in the figure.
The LCD is interfaced to the PORT of the microcontroller to display the information or data.
A transistor driven buzzer is connected to the 24-pin of the microcontroller to give alarm for authentication. The pushbutton switches are connected to 1, 2, and 3input pins of the microcontroller for informing about the type of operation to the microcontroller including scanning, adding and deleting fingerprint.
The relay is connected to the 25th pin of the microcontroller through a transistor to operate the loads or devices. The Microcontroller is programmed in embedded C language in Keil software and this hexa code is dumped to the microcontroller using a hardware circuitry.

Circuit Operation:
In this circuit, for powering the entire circuit, mains AC supply at 230V is stepped down to 12V AC, rectified to DC, filtered and regulated to circuit operating range 5V. This power block is not given in the above circuit for not making a whole circuit complex.
For required operation by user like identifying, adding and deleting finger, an appropriate switch has to be pressed. For certain button pressing, the microcontroller processes the fingerprint images. When a person presses the finger on fingerprint scanner, it gives high and low-logic digital signals to the microcontroller after pressing switch 2. This controller is programmed in such a way that it stores the digital data. When the switch1 is pressed, again it ask for fingerprint scanning; if this data matches with the previously stored fingerprint data, it generates an output signal to the transistor and also displays the information on the LCD display. If the transistor is activated, it automatically energizes the relay coil, and thus the relay gets operated and the corresponding device is turned on. This also gives an alarm from a buzzer upon authenticating the fingerprint. It is also possible to delete the scanned finger by pressing the switch3, and also, if any unauthorized person tries to access the device, this system gives an alarm. This system can be implemented at homes since it is affordable to generate home alarm system. This type of authentication for controlling devices and appliances is highly secured and more reliable at a lower cost due to inexpensive microcontroller. Thus, you might have got an idea of implementing a fingerprint authentication system by using a simple controller. This can also be implemented as an Attendance system in schools and offices by adding external memory.

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

Result

By using this project the design and implementation of ID authentication system based on Fingerprint Identification is designed, and finally, the problem at hand, which is exam student impersonation and corruption in Tertian Education will be demolished and to demonstrate that anything can be achieved using computer technology in this fast growing Information Technology and computer communication world . Simulation phase of this project has been achieved, with the following devices: Microcontroller (At mega 328), LCD display device (LM016L), regulated DC 5V power supply, Keypad-, Virtual Terminal, X1 Crystal clocking, for the devices operations. Microcontroller, this is the heart of the whole system, it is there to facilitate the connection between devices, control the operation of every device connected on this system, it has clocking equipment that must be synchronized with the crystal clocking device to ensure precise operation of the system. Keypad, this device is used as input device used by the user (student) when they are entering their password during authentication process. LCD display is used as the output device of the whole system because, every message that the system need to convey to the user, is display on here, starting from displaying the name of the system (Biometric Fingerprint based exam authentication), asking the user to place their fingers (Put your finger), displaying the results of the authentication (Enter the passkey or Access denied student not registered) and the final display if the user's ID is correct (Access granted). Variable resistor, this is to give brightness to the LCD display. Crystal Clocking, this has the simple task, which is to provide clocking to the system, clocking which is synchronized with the clock of the microcontroller. Virtual Terminal is used as input device as well to input the student number of the student when the system ask the user to put their finger, because there is no fingerprint scanner on the system, so this device is used in the simulation phase. And the final devices are the capacitors, which are used to prevent the unwanted current from entering the system.

Pictorial operational display of the project work is shown in the steps below:

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

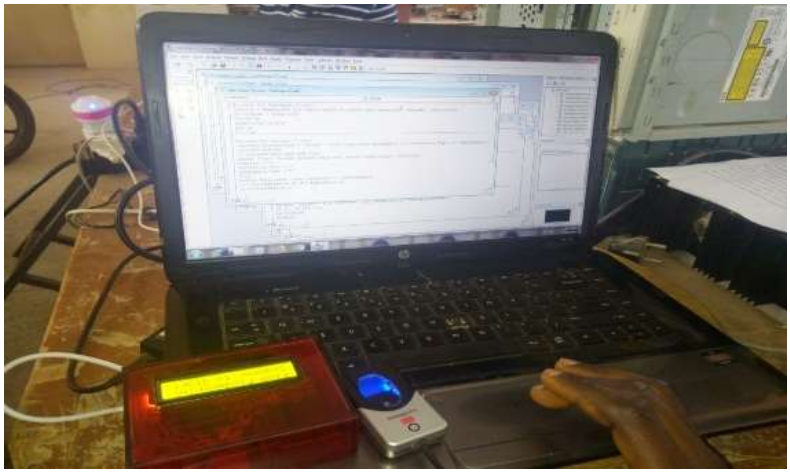

Plate 1*: First screen display after the launching of the software*

Plate 2*: The Start up page where you will be required to select the type of finger print scanner you will want to use that are supported by the design*

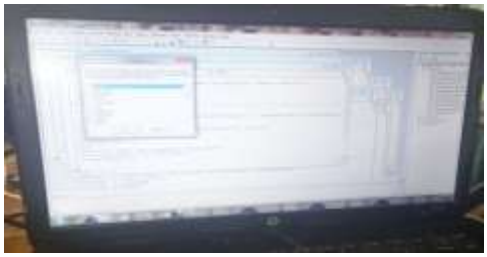

Plate3*: Welcome page after the above step*

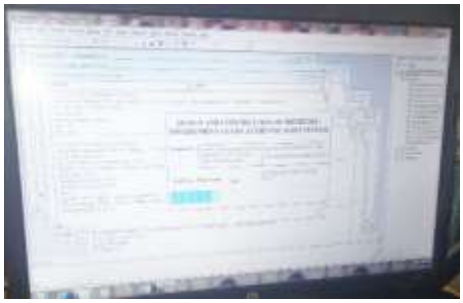

Plate *4: Log in page*

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

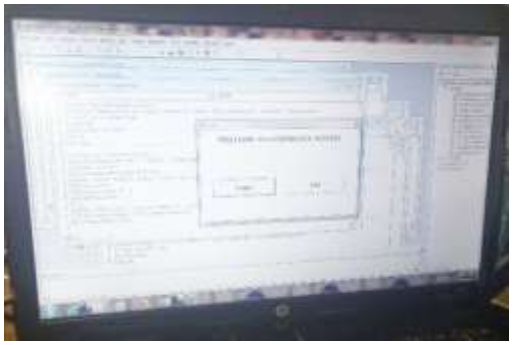

Plate *5: in this step, the admin will be required to log in his user name and password*

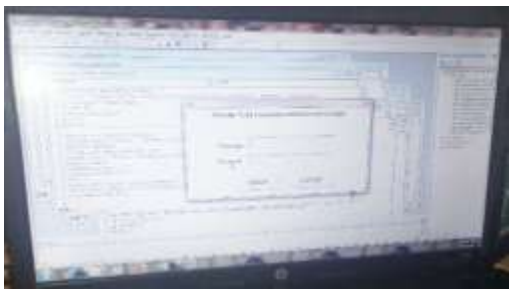

Plate *6: After the login in by the admin, a dialogue box will appear to display successful log in or display error in log in*

Plate *7: login successful*

Plate *8: verification stage*

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

Plate *9: registration stage*

Plate *10: registration successful, access granted*

Plate *11: list of register course*

Plate *12: Name of the course written by the register student*

INTERNATIONAL JOURNAL – ERT
VOL. 10 NO.5 DEC-2019 ISSN: 1074-4741

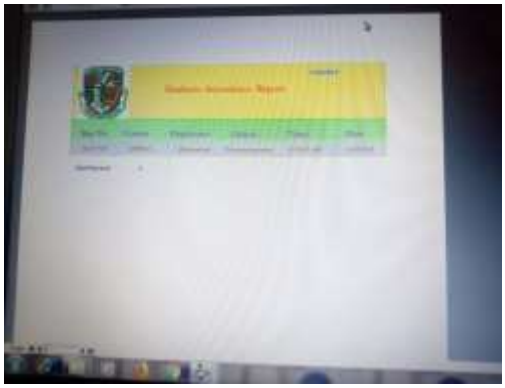

Plate *13: Student's attendance report*

Analysis

Although it was not an easy job, to prove that the proposed system is working according to how the real systems work. This was proved by implementing the project in simulation but its working according to the way it is intended to work. By simulating this project one will see the display on the LCD, the system writing the name of the project " Biometric Fingerprint Exams Authentication", few seconds later it will display the following message: "CLICK ME " this is just to tell the subject (student) to be authenticated to put her/his finger on the fingerprint scanner for it to be able to read his/her fingerprints, after that if the student is authenticate then the following message will be displayed: "ENTER YOUR IDENTIFICATION NUMBER", this is a password that every registered student got during registration/enrolment phase, and if the password entered is correct then access is granted, so the following message will be displayed on the LCD display: "WELL DONE LOGIN SUCCESSFUL". Furthermore, if the student is not authenticated then the system will never ask the student to enter the passkey, but will display the following message: "ACCESS DENIED STUDENT NOT REGISTERED" which means that particular student is not in the system, he/she is not registered.

Conclusion

In this project a Biometric Model for Examination impersonation and Biometric Access is a better substitute for the use of Identity card in verifying users 'identity Experience has shown the porosity of Identity cards in uniquely identifying individual in the face of sophisticated Forgery technology. The naturalness in the use of fingerprint makes it a reliable access control technique. The fact that a user no longer needs to carry identity cards and other documents for identification explain the ease of use of the exam hall authentication system using fingerprints.

The implemented minutiae extraction is much more accurate and faster than our previous feature-extraction

REFERENCES

Cheng K. L., Xiang T., Hirota, and Ushijimaa K., "Effective Teaching for Large Classes with Rental PCs by Web System

Chikkerur S .S., "Online Fingerprint Verification System" M.Sc. Thesis. SUNY: Buffalo, NY, 2005

Kadry S., and Smaili M., "Wireless Attendance Management System Based on Iris Recognition" 2010

Kamaraju M., Kumar P. A., Krishna B. A. and Rajasekhar B, "Embed-de Fingerprint Recognition System", Recent Researches in Telecommunications, Informatics, Electronics and Signal Processing, 2013

Nawaz T., Pervaiz S., and Azhar-Ud-Din A.K., "Development of Academic Attendance Monitoring System Using Fingerprint Identification".2009

Pankanti S., Prabhakar S., and Jain A.K., "On the Individuality of Fingerprints". IEEE Transaction on Pattern Analysis and Machine Intelligence.24(8), 2002

Shoewu O. and Badejo O., "Radio Frequency Identification Technology: Development Application and Security Issues". Pacifi Journal of Science and Technology. 7(2):144 152,.2006

Shoewu O.O, Olaniyi M., and Lawson A., "Embedded Computer-Based Lecture Attendance Management System". African Journal of Computing and ICT (Journal of IEEE Nigeria Computer Section). 4(3):27 – 36, 2011