

DEVELOPMENT OF AN ENHANCED FINGERPRINT BIOMETRIC BASED ATTENDANCE MANAGEMENT SYSTEM

Nwabudike Uju Cynthia
nwabudikecju@gmail.com

Umeasiegbu T

Computer Science Department, Chukwuemeka Odumegwu Ojukwu University, Uli

ABSTRACT

In multitude of academy institutions and establishment, student and employee attendance is taking seriously as most management frown at absenteeism and sanctions the individuals involved. Generally, the approach of attendance taking used to be manually using a physical booklet as register. This process is susceptible to manipulation and impersonation. The attendance register could get destroyed, robbed or misplaced. So, numerous electronic approaches were advanced to counter some know short coming typical with the traditional method. These consist of Bluetooth, clocking machine and Face recognition, etc. While the clocking machine and RFID techniques could not solve the problem of impersonation accurately, some human fear the health implications of the use of biometrics like iris and facial scanner. Fingerprint scanning is the most acceptable biometric approach with the ability to eliminate all the problematic spots outlined so far, despite this, computer support is always needed. The process advanced utilizes a portable fingerprint scanner as the input to acquire fingerprint images and a notebook mobile terminal for the processing of the images and records attendance. The Object Oriented Analysis and Design (OOAM) is used in the analysis and design of the proposed system. The class attendance management system is developed using JAVA as front end and mySQL as backend for storing students' information and attendance records. Experimental results showed that the developed system was able to eliminate the problems associated with manual method as well as prevent students' from signing attendance for fellow colleague.

Keywords: Biometric, Fingerprint, Attendance, Scanner

I. INTRODUCTION

Academic attendance for both students and lecturers are very vital since it will affect the students from gaining knowledge and skills as well as their grades. This paper is about the students and lecturers attendance system through the matching of their fingerprint to confirm their attendance. The main purpose of this paper is to develop desktop-based application that will enable the attendance of both students and lecturers by fingerprint, there is one and only one fingerprint occurrence in the world for each person which will never has duplication. So, fingerprint biometric attendance system is known as the best authentication approach when it is concerned with students/lecturers attendance record. In addition, due to advancement in technology it is not unusual anymore to take the attendance via fingerprint.

Nowadays, most universities and colleges are still using the traditional attendance system which requires student to sign on a piece of paper every time they attend a class throughout the whole semester. Using the traditional attendance system, we can obviously see that there are few problems such as it will be no backup for the attendance records once the lecturer accidentally lost the attendance sheet, course mate help those who did not attend the class sign the attendance which also known as buddy-signing as well, hard in analyzing and tracking student performances based on attendance factor, student lack of knowledge and skills due to the poor attendance in attending classes, and etc. It is important to overcome these problems since it will help in improving the academic performance of students as well as the teaching environment of the lecturers.

II. Related Work

Fingerprint technique for biometric verification is one of the primeval known biometric techniques known but still the most widely utilized due of its easiness and good records of accuracy. It is a well know fact that every individual is born with a different pattern on their fingers and these features are utilised to determine and differentiate between two different persons, even for an identical twin.

The enormous achievement of this fingerprint biometric method in an educational institute or organization cannot be overemphasized. The fingerprint recognition and verification approach has been utilised to replace the conventional method as it saves time and eliminates the entire shortcoming know with the traditional attendance register booklet. A fingerprint scanner and the computer terminals need to be located in the classroom, and both the lecturers and students would be mandated to place their finger on the fingerprint sensor so as to indicate their presence in the class. The records are hoarded in the database for authentication. The moment a finger is placed across the scanner, verification would be carried out for the student (Acharya et al, 2010).

The attendance system is accomplished using the Fingerprint technique and a notebook computer. The Fingerprint approach aid as a personality affirmation during the attendance taking process. The scanner scans the form from the fingerprint module and verifies this data with the already secured pattern in its database. If the information present in the database is same with the stored fingerprint, the system marks the attendance. If the finger information does not return a match with the data stored in the database, an alarm will be set off to notify the security personnel to take necessary action. The system is developed in such a way that it is interfaced with a computer either to print out the attendance or to get more elaborate information of the people whose attendance is taken (Acharya et al, 2010).

The trending interest in this modern world is concerning national security, recognizing theft as well as on-line terrorism. Investigators specify Biometric as a solution for identify user's personality and security threat exude in this modern day. Biometric recognition is any automated quantitative, sturdy and unique physical features or personal trait that can be used to recognizing an individual or authenticate the allege character of an individual. Biometric science uses the quantitative of a person's behavioral features (keyboard strokes, mouse movement) or biological characteristics (fingerprint, iris, nose, eyes, jaw, voice pattern, etc). It is the characters captured that is being converted digitally

into a template. The identification software can then be used to reveal an individual as the person they claim to be. Fingerprint identification is the widely used biometric method used in the verification of an individual (Saraswat, 2010).

Biometric is an area of technology that utilizes approach for recognizing and authenticating an individual based on physiological and behavioral characters. Because some parts of the human body is use in biometrics, the controversy of getting vanished is not possible and for password to be simply guess can be easily eliminated. Also, utilizing biometrics in many instances can be said to be more effective when speed is of interest and beneficial than using password and ID cards approach.

Utilizing a particular individual fingerprint as a form of verification is just like using natural physical data as a password. The advantage of using biometric verification is that it is absolutely different from each individual. There are no two different persons with the same fingerprint; it is cumbersome and impossible for one another to have the same fingerprint. Also, a fingerprint can never be infer by a fraudulent person, such as a password which imposter can easily predict using a user birth date or any other common password (Pankanti et al, 2002).

Fingerprint can be categorize as one of the most mature biometric features and is recognized in courts of law as a legalize validation of evidence. Fingerprints are used in forensic analysis worldwide in probe of criminal. Most recently, there are growing numbers of persons and commercial users that are presently using or firmly putting into thoughtfulness of using fingerprint-based verification for no any other reason other than the matching performance biometric technology has demonstrated as well as a better understanding of fingerprints.

The author in (Rishabh, 2011) proposed the use of a computerized attendance system, which can eradicate human interference, human data entry error, and repetitive work. This system is going to enhance productivity, lower payroll bug, and lower payroll inflation, lower overtime, retirement of legacy systems, Eradicate of paper costs, and which can provide all the reports on demand. In this system, faculty has to take attendance manually, only these records have to be inputted into the computerized system. But in this also, the problem of data entry error may persist.

RFID reader was designed with microcontroller, transceiver chip, serial communication IC, LCD, USB interface, power supply module, etc as components. When a staff touches the card reader with their card the data is transfer to PC manager application which will authenticate the data and extract information like staff ID and access time into the database. Again same problem as above system is being faced by this research (Seifedine et al, 2010).

The authors in (Ramnarayan et al, 2013) proposed a system in which a student touch the reader and it transfer the data to the microcontroller for comparison check with the ID already stored in the microcontrollers memory; if ID exist the name, ID and attendance will be displayed on the LCD then send the data to PC via RS323 port. Also, the authors in proposed another system based on RFID where the RFID terminal read the student ID, date and time; and store it into a database in an online server. The problem in this research is that verification is not done. So proxy attendance may be marked.

This work implemented student attendance using fingerprint biometric, as well as taking the attendance of the lecturer during each lecture. The project work also provide a means for taking the attendance for excused students and also places a time frame for taking attendance.

III. Analysis of the proposed System

The System was categorized into three (3) major subsystems which are; admin subsystem, and lecturer subsystem and student subsystem. Each of the listed subsystems above has a different user privileges to use the system.

Admin subsystem, here the user of this subsystem has the following privileges; add/delete/update records and information of the entire system. This subsystem is further broken down into; add Course, assign course, enroll student (which include fingerprint enrollment), enroll lecturer (which include fingerprint enrollment), and report generation. In the listed subsystems the administrator can delete, add, and update the subsystem information.

Lecturer subsystem, unlike the admin subsystem here most privileges are taken away, the user can only activate attendance, view a student record or marked attendance or the courses he/she was assign to lecture on. The subsystem is further broken down into; (I) course (II) lecture taken (III) activation duration.

Student subsystem, here the user of the subsystem has the privilege of taking attendance, this is done by the students placing his finger on the fingerprint scanner surface, and the fingerprint would be processed by the fingerprint scanner. The fingerprint pattern that has been obtained would be compared against the stored enrolment template that is already stored in the database where the enrolment process was executed. When the fingerprint pattern passes the comparison process, it ticks the student present, else it returns fingerprint not found.

The fingerprint acquisition process can be divided into three parts, there are:

- i. The enrolment process
- ii. The verification process
- iii. The data collection process

The enrolment process is carried out once for each person. Each person would be needed to register their fingerprint pattern by placing his thumb finger on the fingerprint scanner. The scanner takes the image of the finger and determines the unique characteristics of the fingerprint image. The fingerprint contains ridges and valleys which have different kinds of breaks and discontinuities. It is the various ridges and valleys that form the basis for the loops, arches, and swirls that are easily seen on fingertips. After the capturing of the ridge pattern of the fingerprint, a template is created, and the fingerprint is encrypted into series of numbers. These series of numbers will be different for each fingerprint pattern. After the process must have been completed, the fingerprint scanner sends the result of the encryption to a memory location or database. The process algorithm is shown in figure 1.1.

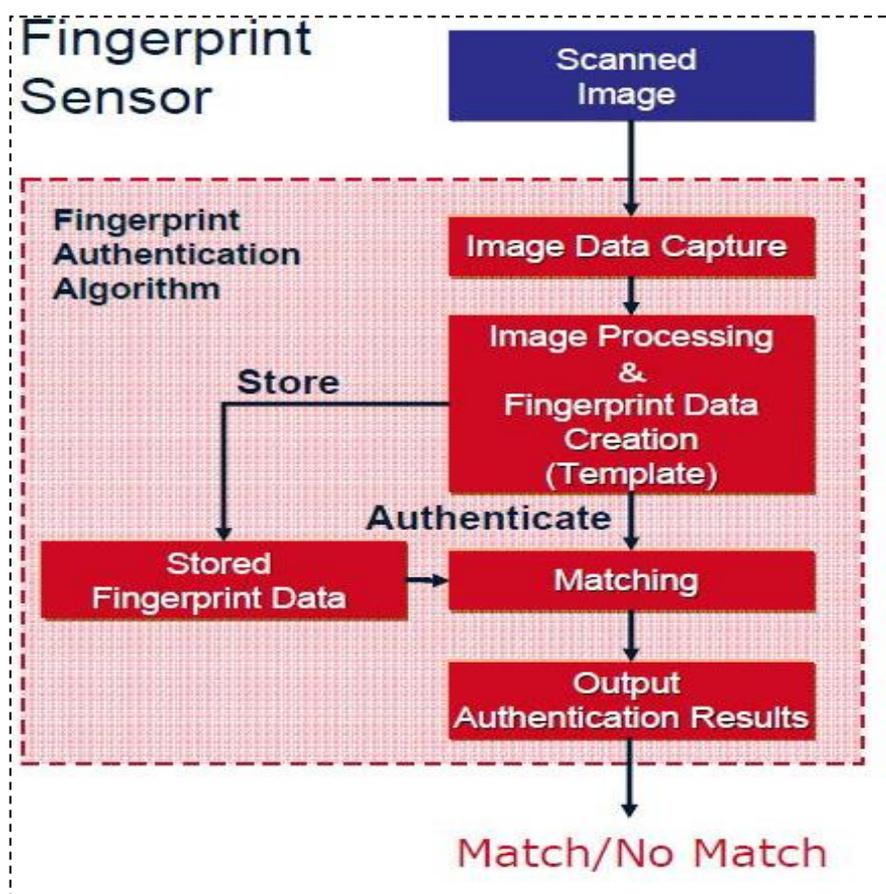


Figure 1.1: Fingerprint sensor algorithm

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 fingerprint 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 comparison process, it shows an acknowledgement in its display and grants the user access.

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 record to know the attendance of a person or to know the number of times a restricted.

IV. Attendance Management Approach

This part explains how students and lecturers will use this attendance management system. Following points will make sure that attendance is marked correctly, without any problem:

- (1) All the hardware will be inside classroom. So outside interference will be absent.

(2) To remove unauthorized access and unwanted attempt to corrupt the hardware by students, all the hardware except fingerprint scanner could be put inside a small cabin. As an alternate solution, we can install Closed Circuit Television (CCTV) cameras to prevent unprivileged activities.

(3) When Lecturer enters the classroom, the attendance marking will start. Computer software will start the process after inputting fingerprint of Lecturer, which takes the attendance of the Lecturer. It will find the Subject ID and Current Semester using the ID of the teacher or could be set manually on the software. If teacher doesn't enter classroom, attendance marking will not start.

(4) After some time, say 20 minutes of this process, no attendance will be given because of late entrance. This time period can be increased or decreased as per requirements.

(5) At the end of the lecture, the lecturer manually marks the attendance of those that took permission.

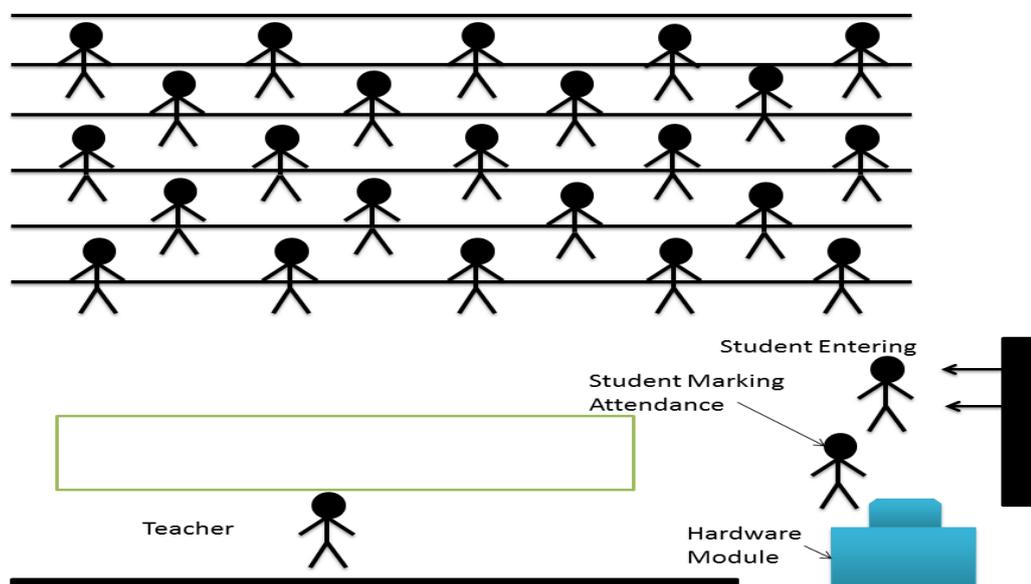


Figure 1.2: Classroom Scenario

V. CONCLUSION

Biometric technology is an effective tool for authenticating identity and discovering fraudulent activities. Analysis have authenticated that biometric data can be utilised in confirming the particular characteristics of a user. Expanding the range of biometrics will heighten the ability to discover humbug matters as it concerns attendance of both Student and Lecturer during lectures. This paper has successfully presented an authentic, dependable, fast and effective system replacing a manual and unreliable system. Also including the time constrain will help in checking lateness to class. This system can be implemented in many institutions especially in the academic institutions for better result regarding the management of attendance of both Students and Lecturers. This system will save time, reduce the amount of work the administrator has to do and will replace the stationery material with an electronic

device. Hence, a system with expected results has been developed but there is still room for further improvement.

VI. RECOMMENDATION

The capabilities of the system can be further improved through the following recommendations:

1. The system can be made wirelessly (through the use of Bluetooth, Wi-Fi, WLAN) so the system administrator can access the attendance information without physically connecting to the Computer system.
2. The system can be interfaced with a GSM Module to send SMS to the Security Personnel anytime an unregistered finger tries to sign-in or out or to parent notifying him/her of his/her child's attendance records.

VII. REFERENCE

- Abhishek, J. (2011). Classroom Attendance System Using Facial Recognition System. A Journal of Forensic and Pattern Matching, 17(1):84-86
- Acharya, D., & Mishra, A. (2010). Wireless Fingerprint based Student Attendance system, National Institute of Technology Rourkela. Retrieved from <http://ethesis.nikl.ac.in/1765/>
- Pallavi, V.(2013). Wireless attendance management system based on iris Recognition. Scientific Research and Essays Vol. 5(12), pp. 1428-1435, ISSN 1992-2248.
- Ramnarayan, S. & REDDY, D. (2013). Student Attendance Tracker System in Android. International Journal for Engineering Applications and Technology (IJFEAT),pg-[119-124], ISSN: 2321- 8134. 22
- Rishabh, M. (2011). An NFC Supported Attendance System in a University Environment. International Journal of Information and Education Technology, Vol. 4, No. 5, DOI: 10.7763/IJET.2014.V4.448
- Saraswat, C. (2010). An Efficient Automatic Attendance System using Fingerprint Verification Technique. International Journal on Computer Science and Engineering. 2(02):264-269
- Seifedine K., & Mohamad, S. (2010). Wireless attendance management system based on iris Recognition. Scientific Research and Essays Vol. 5(12), pp. 1428-1435, ISSN 1992-2248. 21.