DESIGN AND IMPLEMENTATION OF A BIOMETRIC AUTHENTICATION AND VERIFICATION SYSTEM FOR SCHOOLS AND COLLEGES

[1]Mgbeafulike Ike J and **[2]Ndigwe Chinwe**
ike.mgbeafuike@gmail.com franchy_dex@yahoo.com

[1,2] Department of Computer Science, Chukwuemeka Odumegwu Ojukwu University, Uli.

ABSTRACT
Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database. This study aims to design and development of a biometric authentication and verification system for students of universities and colleges. The methodology used in designing and analyzing the system is Object Oriented Analysis and Design Methodology (OOADM).The new system utilizes a portable fingerprint scanner as the input to acquire fingerprint images and notebook personal computer as the mobile terminal for the processing of the images and records attendance. It also includes a database to store student's information and attendance records. Visual Basic.net was used as the programming language to develop this system and Microsoft Access was used as the database management system for the new system. The attendance monitoring system will be used to monitor attendance of the student and eliminate ghost students from the institution. It will eliminate the problems of manual method and help in detecting fraudulent students in the school system. The system was tested and found working correctly.

Keywords: Biometric, authentication, verification, scanner, attendance

1.0 INTRODUCTION

Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database, At the moment, we are living in an extremely small world. Individuals are highly mobile, constantly connected to each other, and their daily lives are highly influenced by the information technologies in particular mobile devices and social networking. In such societies, most of the services are delivered electronically via intelligent machines that can be accessed remotely. These include banking, e-commerce, governmental-services to citizens, hotel booking, social aides, and many other fields related to work, traveling, defense, education, business and social relationships.

1.1 The identification problem

Services are now much easier and more immediate. The consumption of the services is generally based on the client-server paradigm where the machine is the server and the client is the individual user. Security of such systems must be highly considered, since the service must be delivered only to legitimate user who has to be initially identified. Traditionally, these systems used, and still are, classical authentication schemes based on credentials consisting in secret information (such as passwords) and/or possessed tokens (certificates,

smartcards). Unfortunately, such systems are not enough secure since credentials can be forgotten, stolen or duplicated. In fact, serious concerns revolved around the security of such systems since their vulnerability has been widely exploited by malicious persons to get fraudulently access to privileged rights. These fraudulent incidents are with limited scale in countries such as Algeria where e-services are in their first stages; however, it is reported that over 17 million of US persons were victims of one or more incidents of identity theft in 2014 (Harrell & Langton, 2015). Statistics confirm that governmental and big private organizations are the most targeted ones. The number is growing year after year. Three main actors could be determined to be responsible for such inconveniences, i) the user is being accused of not taking enough care to protect his credentials, ii) the hacker who has exploited the carelessness of the user as well as some security flaws in the system, and iii) the security strategy adopted by the identification system. It seems that the system shall be liable for most associated security failures since it has to take into consideration the two first lacks. In fact, the identification strategy adopted is not related to the user himself, rather it is based on what he shall know or what is in his possession. This is the main source of vulnerability and the subsequent security issues. The establishment of identity problem is not limited to e-services systems only, it is particularly encountered in controlled areas such as airports, traveling stations, governmental and private premises where individuals should be identified based on some collected data. The issue arises acutely in forensic applications where corpses must be identified and crime evidences must be collected. It is very clear that the classical identification systems are useless in such situations. In any cases, governments, private organization as well as individuals are deeply concerned about the growth of identity scams. Some of the problems encountered in the current system of students' verification and identification are:

i. Student impersonation
ii. Insecure authentication of students
iii. Inefficiency of the process due to students' population or size of a class
iv. The tedious nature of the manual process

Stronger identification and verification mechanisms are of major priority.

Biometrics is a method to provide reliable identification of individuals. Biometric technology measures physical or behavioral characteristics to determine the true identity of a person. While just a few years ago biometrics were mostly the domain of science fiction, this technology is now mature and used in an increasing number of settings. Biometric systems can broadly be classified into two categories based on the respective biometric characteristics: biological and behavioral. • Biological characteristics are the physical characteristics of body parts, such as fingerprints or hand contours, i.e. characteristics that do not change substantially over a person's lifetime. • Behavioral biometric systems analyze a person's behavior and actions. Examples of monitored behaviors include signature movements or voiceprints. It should be noted that behavioral biometric characteristics also have a physical component, e.g. the articulatory system in the case of speech (Jain et al, 2000).

There are two types of system, which help automatically in establishment of identity of a person:

i. Authentication (verification) systems
ii. An identification systems

In a verification system, a person desired to be identified submits an identity claim to the system, usually via a magnetic stripe card, login name, smart card, etc., and the system either rejects or accepts the submitted claim of identity (Am I who I claim I am?). 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?). Biometric verification is the process of confirming a claimed identity through biometrics. The decision is therefore binary, answering the question: 'Based on the data presented – can it be assumed that this subject is the rightful owner of the identity claimed?' Depending on the individual use case, this confirmation can be achieved by comparing the biometric trait presented by the subject to a template stored either locally or remotely.

Biometric authentication is a security process that relies on the unique biological characteristics of an individual to verify that he is who is says he is. Biometric authentication systems compare a biometric data capture to stored, confirmed authentic data in a database.
The aim of this research project is to design and implement a Biometric Authentication and Verification System that can be used for the purpose of recording the biometric details of the students in a classroom in order to be used in the identification and recording of student attendance in classrooms.

The objective to be achieved at the completion of this research includes the following:

- To create a system that can collect the fingerprint details of the students in a class
- Register the students using their collected biometric information
- Enable the students to mark their attendance by using their fingerprints
- Display the attendance records for the students to the lecturer.

2.0 RELATED WORK

2.1 BIOMETRIC TECHNOLOGY

Biometrics refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometric identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities. A number of biometric traits have been developed and are used to authenticate the person's identity (Babich, 2002). The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc. Different types of biometrics are used in any identification system, such as DNA Matching (Chemical Biometric), Ear (Visual Biometric), Eyes (Iris Recognition and Retina Recognition), Face Recognition (Visual Biometric), Fingerprint Recognition (Visual Biometric), Gait (*Behavioral Biometric*), Signature Recognition **(**Visual/Behavioral Biometric**),** Voice (Speech and Speaker Recognition), etc (Biometrics Institute Limited, 2018). A biometric system can be either an 'identification' system or a 'verification' (authentication) system. Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database. Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

There are some existing related works on the application of different methods in managing attendance of students. One of the methods proposed for monitoring attendance is embedded computer based lecture attendance management system. In this type of system, a card is reader is interfaced with a digital computer system and an electronic card is provided and personalizes to each user for authentication. They used a wireless attendance management system that authenticates using the iris of the individual. The system uses an off-line iris recognition management system that can finish all the process including capturing the image of iris recognition, extracting minutiae, storing and matching.

Attendance Management has also been carried out using attendance software that uses passwords for authentication. The authors designed and implemented a system that authenticates the user based on passwords, this type of system allows for impersonation since the password can be easily fiddled. There are cases where passwords could be forgotten which in turn prevent the user from gaining access into the system.

There are attendances software's that are device centric solutions such as RFID-based student attendance system and GSM-GPRS based student attendance system. The GSM-GPRS based systems works by using the position of classroom for marking attendance which is not dynamic. Wrong attendance might be marked if schedule or location of the class changes. One of the problems with RFID based systems is that students will be compelled to always carry RFID cards and also the RFID detectors are needed to be installed. Automated Teller Machine(ATM) system authentication using fingerprint Biometrics in the banking sector is a related study to this Personal Authentication System using fingerprint biometrics of students in institutions, where the students biometrics data are been collected in their various class, laboratory, examination halls and even tutorial by their lecturer, invigilators and even securities personnel in the institution to keep track of each student's attendance performance in various courses. This biometrics authentication can also be used in the banking sector to keeping track of all activities been carried out by each customer that performs transaction through the ATM. With an ATM, a customer or client is able to conduct many banking activities such as cash withdrawal, paying electricity & phone bills, money transfer, beyond official hours and physical interaction with bank staff (Mashurano, 2013).
A newer high-tech method of operating sometimes called card cloning to entangle the installation of a magnetic card reader over the ATM's card slot & the use of a wireless surveillance camera to keep the user's Personal Identification Number. Real Card data are then cloned into a duplicate card & the criminal attempts to cash withdrawal. To overcome this piracy in money transactions, the idea using fingerprints of customers as password along with the traditional pin number (liqiang, 2013).

2.2. AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

By the 1970s, computers were in existence, and the FBI knew it had to automate the process of classifying, searching for and matching fingerprints. The Japanese National Police Agency paved the way for this automation, establishing the first electronic fingerprint matching system in the 1980s. Their Automated Fingerprint Identification Systems (AFIS) (Moses et al,. 2010), eventually enabled law enforcement officials around the world to cross-check a print with millions of fingerprint records almost instantaneously. The Automated Fingerprint Identification System (AFIS) is a computerized storage system for millions of fingerprint images. The AFIS is an effective system for identifying people and establishing the criminal history of offenders. The Automated Fingerprint Identification Systems (AFIS) includes two processes, fingerprint identification and verification. The Automated fingerprint identification is the process of automatically matching one or many unknown fingerprints against a

database of known and unknown prints. The Automated fingerprint verification is a closely related technique used in applications such as attendance and access control systems. On a technical level, verification systems verify a claimed identity whereas identification systems determine identity based solely on fingerprints The biometric authentication is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process (Kumar et al., 2012). During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrollment. Here the processed sample is stored in a storage medium for future comparison during an authentication. A new automated approach is needed to (i) extract each fingerprint image (ii) process each of these images to produce a reduced template of characteristic information, and (iii) search a database to automatically produce a highly reduced list of probable candidates (Cole, 2001).

3.0 The Proposed System

The proposed system, biometrics authentication system is an application which depends on the input from a biometric machine for validation and authorization of students'. The proposed system will help check increasing crimes of student absent from classes and keep biometric records of all students. All it takes is to access the application; it involves the finger print of the student and the student's personal data, such that when it is being submitted, the system will validate it with what is stored in the database. If it matches, then it authorizes attendance marking, if it does not match, it will attendance marking.

3.1 GOALS AND THE FUNCTIONALITIES OF PROPOSED SYSTEM.

The proposed system is a digitally powered computerized biometric authentication system comprising two major components. Namely, hardware and software.

The hardware comprises of personal computer system, a thumb scanner, and a system camera, internet service facilities. The software consists of a digitally mastered database system, a user friendly interface and internet server software.

Owing to the above mentioned facilities the proposed system shall emerge as "modern biometric facilities equipped with the following capabilities.

Effective Students Registration: They will be capable to register thousands of students with ease and efficiency. This will render the manual registration process unnecessary.

Database Management: The database system of the proposed system is highly efficient and digitally powered, which will automatically address the problem of multiple entries and safety of data.

Biometric Data Capture: The biometric data collected during registrations will make screening process more authentic and easier. No student can be mistakenly identified as far as "thumb print" is concerned.

Authentication Number: An automatically generated authentication number will be given to each student immediately after screening. This code number helps to dissuade student's material outside the exam hall.

Note that, the biometric thumb printing technology will make it impossible for any illegal students to gain access to examination hall thereby eradicating the problem of impersonation as well as security threats.

3.2 SYSTEM ARCHITECTURE

The operational architecture for the proposed system is illustrated in the figure below:

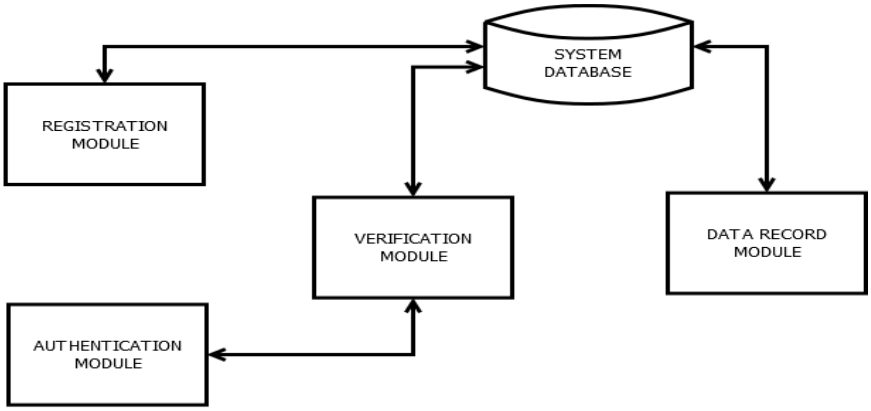

Figure 2. System Architecture

From the diagram it can be seen that the system is made up of the following modules:

Registration Module: This is used to register the student details such as biometric and personal data.

Authentication Module: This is used to enable the user of the system access after the submission of the correct authentication details.

Verification Module: This is module that is used to verify the students in attendance for the lecture

Data Record Module: This is used to record the attendance records of the students in the system database.

Database: This is the database used to store information for the system.

Implementation

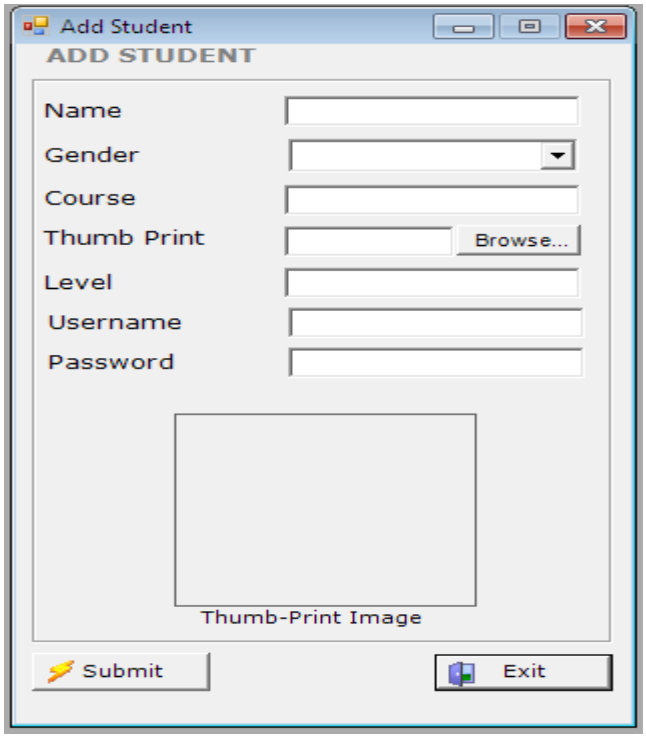

Figure 3. Student Registration Form

STUDENT ATTENDANCE MODULE

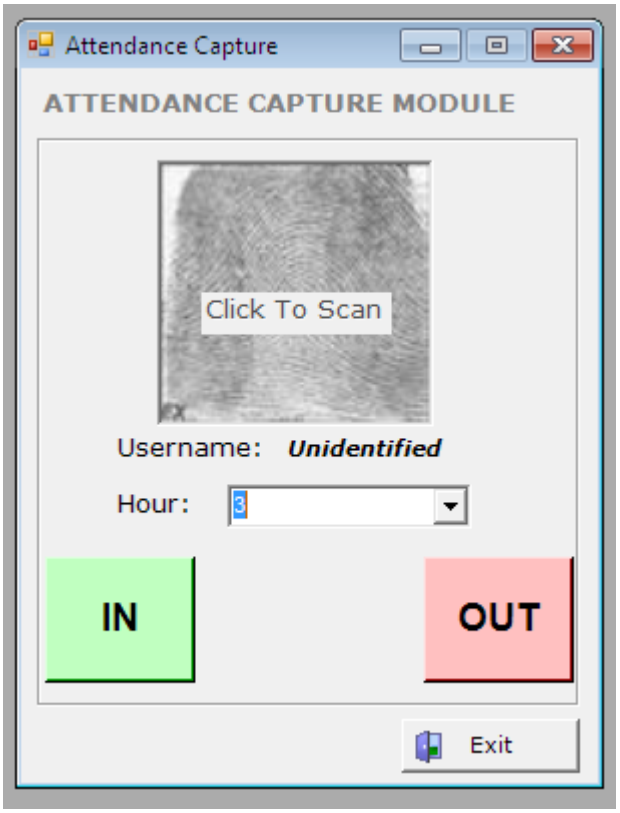

Figure 4. Student Attendance Module

This module is used by the students to record their attendance using biometric information provided by the students.

4.0 CONCLUSION

Traditionally, students' authentication during class and examination is done in the conventional way (username and password). Therefore, the implementation of an electronic biometric method of authentication will greatly assist institutions and organizations thereby prevent time consuming process. Employing a more simplified, reliable and efficient model for authenticating students writing electronic examinations based on biometric is formulated and implemented. This system provides both the students and administrators with ease of access to information needed as well as monitoring of the students by the administrators. This will increase the productivity of institutions and organizations. Experiments were conducted using SecuGen fingerprint reader to capture live image of students and image enhancement was performed using crossing number concept to extract the enhanced images so as to improve the image quality. It was coded using Java (NetBeans IDE 7.4) to implement algorithms for enhancement, minutiae extraction and matching processing, where the resulting minutiae information was used as a method for identifying and matching fingerprints. The naturalness in the use of fingerprint makes it a better method for access control as this will dissuade students from carrying identity cards or other known documents for identification and authentication during electronic examinations explains the ease of use.

References

Aleksandra Babich, “Biometric Authentication. Types of biometric identifiers”, Bachelor’s Thesis, Degree Programme in Business Information Technology, HAAGA-HELIA University of Applied Science, 2002.

Biometrics Institute Limited, “Types of Biometrics” Kingsway, London WC2B 6UN, United Kingdom, http://www.biometricsinstitute.org/pages/types-of-biometri cs.html

Jain, A., Hong, L., & Pankanti, S. (2000). "Biometric Identification". Communications of the ACM, 43(2), p. 91-98. DOI 10.1145/328236.328110

Kenneth R. Moses; Peter Higgins; Michael McCabe; Salil Probhakar; Scott Swann, “Fingerprint Sourcebook – Chapter 6: Automated Fingerprint Identification System (AFIS)”, PDF Document, https://www.ncjrs.gov/pdffiles1/nij/225326.pdf, 2010.

Sahoo, Soyuj Kumar; Mahadeva Prasanna, SR (1 January 2012). Mahadeva Prasanna, SR, Choubisa, Tarun. “Multimodal Biometric Person Authentication: A Review”, IETE Technical Review, Vol 29 (1), February 2012.

Cole S, “Suspect Identities”, Harvard University Press, Cambridge, MA, 2001.