TITLE PAGE

EXAMINATION VERIFICATION SYSTEM USING BIOMETRIC
(A CASE STUDY OF WAEC)

BY

ENEH IJEOMA BRIDGET

CST/2009/380

PROJECT REPORT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, CARITAS UNIVERSITY AMORJI NIKE ENUGU

IN PARTIAL FULFILLMENT OF THE AWARD OF DEGREE IN BACHELOR OF SCIENCE (B.Sc) COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

JULY, 2013.

CERTIFICATION

This is to certify that this project work “Examination Verification System using Biometrics” (A case study of WAEC) was carried out by me.

---------- ----------

Eneh Ijeoma Bridget Date

APPROVAL PAGE

This Project is written under the direction and supervision of the candidate's project supervisor and approved. This is to satisfy that the student has presented it orally to the Department of Computer Science and Information Technology Caritas University Enugu in partial fulfillment for the award of Bachelor of Science (B.Sc) Degree in Computer Science and Information Technology.

…… **……**

Engr. Solomon Onuh **Date**

Supervisor

…… **……**

Dr. Arinze Nwaeze **Date**

Head of Department

…… **……**

Dr. Boniface Ekechukwu **Date**

(External Examiner)

DEDICATION

I dedicate this project report to Almighty God whose love and grace towards my academic pursuit is endless and to my parents for their love and contribution.

ACKNOWLEDGEMENT

My profound gratitude goes to my project supervisor Engr. Solomon Onuh and also to my HOD Dr. Arinze Nwaeze for making this project a learning process, others in the trend are my departmental lecturers and a lots of friend in the science field. I also want to acknowledge my parents and my siblings for their great support during academic pursuit; may the Almighty God bless them for me. My great thanks goes to God Almighty who has made this project a success. The good work he has started in my life and I know he will complete it in Jesus Name Amen.

ABSTRACT

My research Project is to develop fingerprint biometrics systems that assist in the elimination of examination impersonation. Up till now, the WAEC examination board (WAEC) is not using fingerprint as mode of identification, this has resulted in people sitting for WAEC examinations for others who collect the result at the end. With the adoption of fingerprint, this will be eliminated as fingerprint; this will be eliminated as fingerprint identification will also be employed during collection of results and certificates. This target can be mainly decomposed into image preprocessing, feature extraction and feature match. For each sub-task, some classical and up-to-date methods in literatures are analyzed. Based on the analysis, an integrated solution for fingerprint recognition is developed for demonstration. My demonstration program is coded using visual studio for the program, some optimization at coding level and algorithm level are proposed to improve the performance of my fingerprint recognition system. These performance enhancements are shown by experiments conducted upon a variety of fingerprint images. Also, the experiments illustrate the key issues of fingerprint recognition that are consistent with what the available literatures say. Main objective is to eliminate any form impersonation during exam by employing a more secured means of fingerprint biometrics.

TABLE OF CONTENTS

CHAPTER ONE

1.0 INTRODUCTION

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, 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 has developed.

The Jesuits introduced written examination into their schools in the 16th century. The Definitive Ratio Argue Institution Studiorum of 1599, which was not revised until 1932, contains a code of rules for the conduct of school examinations, which were held annually, and determined whether or not children were promoted to a higher class. 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:

1) Authentication (verification) systems and

2) 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 data base) without the subject's having to claim an identity (Who am I?). The topic of this paper is channel 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, which use "Something that you know," such as a personal identification number (PIN), or "something that you have," such as an identification (ID) card, key, etc., are no longer considered reliable enough to satisfy the security requirements of electronic transactions or school management system. All of these techniques suffer from a common problem of inability to

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. Although biometrics cannot be used to establish an absolute “yes/no” personal identification like some of the traditional technologies, it can be used to achieve a “positive identification” with a very high level of confidence, such as an error rate of 0.001%. Fingerprint technology using biometrics employ certain advantage of eradicating the problem of examination impersonation by allowing the measure of what you are to perform the security activities of student participation in the exams.

1.1 BACKGROUND OF STUDY

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 qualifications, such as SAT scores, to students. Most exam boards are running as non-profit organizations.

The West African Examinations Council (WAEC) is a not-for-profit examination board formed out of the concern for education in Africa. Established in 1952, the

council has contributed to education in Anglophonic countries of West Africa (Ghana, Liberia, Nigeria, Sierra Leone, and the Gambia), with the number of examinations they have coordinated, and certificates they have issued. They also formed an endowment fund, to contribute to the education in West Africa, through lectures, and aid to those who cannot afford education.

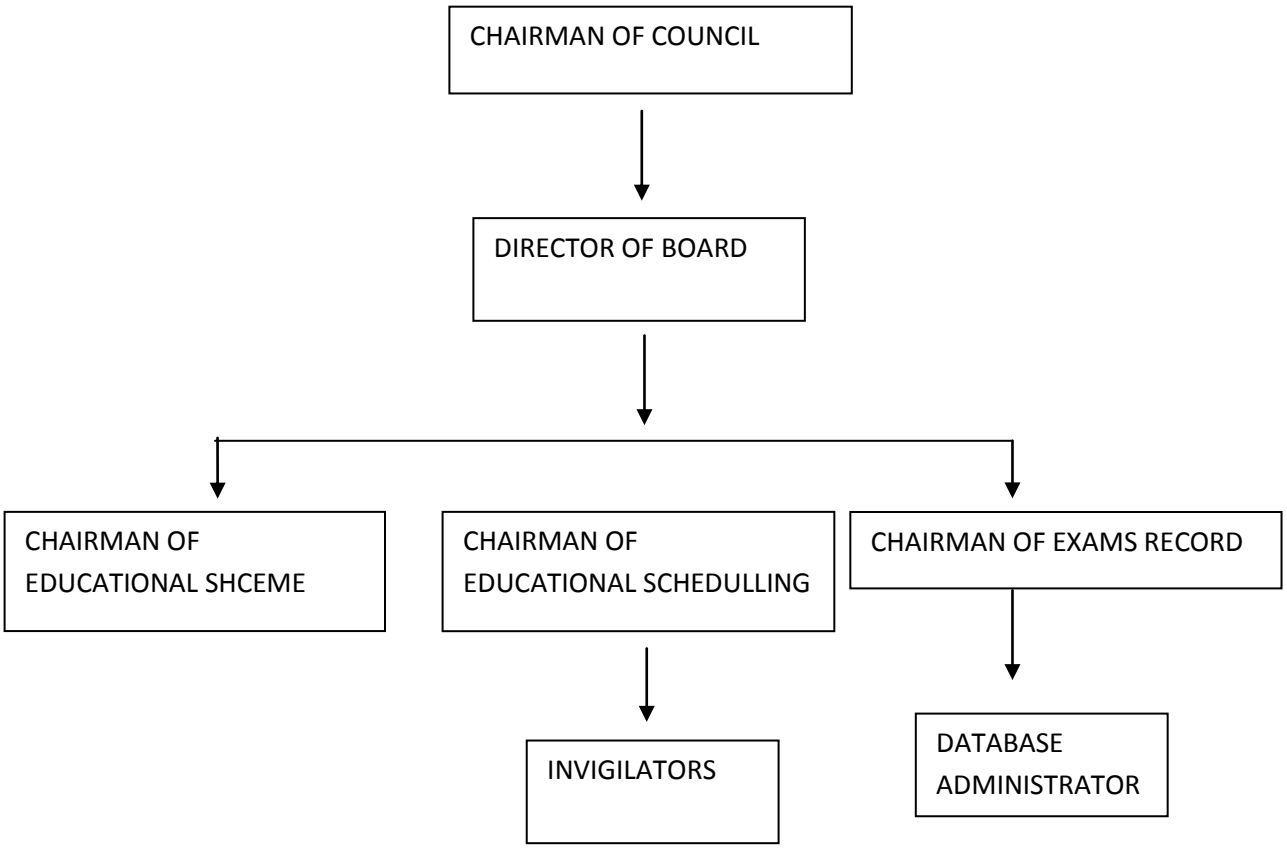
Dr. Adeyegbe, HNO of WAEC Nigeria (2004) said "the council has developed a team of well-trained and highly motivated staff, and has administered Examinations that are valid and relevant to the educational aspirations of member countries". In a year, over three million candidates registered for the exams coordinated by WAEC. The council also helps other examination bodies (both local and international) in coordinating Examinations.

The University of Cambridge Local Examinations Syndicate, University of London School Examinations Matriculation Council and West African Departments of Education met in 1948, concerning education in West Africa. The meeting was called to discuss the future policy of education in West Africa. At the meeting, they appointed Dr. George Barker Jeffery (Director of the University Of London Institute Of Education) to visit some West African countries, so as to see the general education level and requirements in West Africa. At the end of Jeffery's three month visit (December 1949- March 1950) to Ghana, the Gambia, Sierra

Leone, and Nigeria, he tendered a report (since known as Jeffery report) strongly supporting the need for a West African Examination Council, and making detailed recommendations on the composition and duties of the Council. Following this report, the groups met with the governments of these countries, and they agreed on establishing a West African Examination council, fully adopting Jeffery's recommendations.

The legislative assemblies of Nigeria, Ghana, Sierra Leone, and the Gambia passed an ordinance (West African Examinations Council Ordinance NO. 40) approving the West African Examination Council in Dec 1951. The Ordinance agreed to the coordination of exams, and issuing of certificates to students in individual countries by the West African Examination Council. Liberia later issued their ordinance in 1974, at the annual meeting held in Lagos, Nigeria. After the success of forming an examination council, the council called a first meeting in Accra, Ghana on March 1953. In the meeting, the registrar briefed everybody about the progress of the council. In that same meeting, five committees were formed to assist the council. These committees are: Administrative and Finance Committee, School Examinations Committee, Public Service Examinations Committee, The Professional, Technical and Commercial Examinations Committee, and the Local Committee. The total number of people present for this meeting was 26.

ORGANIZATIONAL DIAGRAM



1.2 OBJECTIVE OF THE STUDY

The objective of this study is as follows

- To create a system that is capable of tracking impersonators in the examination system using the methodology of finger print biometrics.
- To reduce rate of corruption in the educational sector and increase the rate of self confidence on students.
- To demonstrate the possibility of computer technology in the satisfaction of human needs and also enforce strict security measures that ensure unregistered students do not write exams for other registered students.

1.3 JUSTIFICATION

The justification for the system is as follows

- To add more security measures to the examination processes using finger print biometrics.
- To eliminate the possibility of an imposter appearing in an exam.

1.4 STATEMENT OF PROBLEM

The problems which are encountered in the previous system are

- Student impersonation
- In secured authentication of students
- Manual verification of student

1.5 SCOPE OF THE STUDY

This system would be implemented using the vb.net and Microsoft access database and also all necessary method of data collection within my reach to ensure the system meet up to acceptable standard has been put into consideration. Also tables' graphs for easily analysis and demonstration of development trend of achievement would also be shown. Also this work would be carried out under close supervision for adequate guidance and interpretation of the work as it unfolds.

1.6 SIGNIFICANCES OF STUDY

With the increasing rate of exam malpractices in the educational sectors the school management deserve to inculcate a tight security means to ensure that these activities of exam impersonators stop. The activities of these exam impersonators have seen the educational sector suffer some serious form corruption ranging from registered student, to examination supervisor. So it best for the educational body to

strategies some certain security means to stop this aspect of corruption in the educational sector.

The system uses a finger prints biometrics this would help ensure that only registered student during registration with their finger prints are allowed into the examination hall.

- The system would contribute in the area of stopping any activity of corruption in the educational sector among students, and student to teachers.
- Hard work would be encouraged as every registered student knows he/she is going to write the exam by him or herself.
- The impersonation which has eating the educational system there by encouraging laziness among students would be eliminated and standard of student educational performance would be increased.

DEFINITION OF TERMS/VARIABLES USED

WAEC: A body responsible for conducting and issuing certificate to secondary school graduating student among West Africa.

DATABASE: A collection of related information which can be stored and retrieved.

EXAMINATION: A measure for the test of knowledge.

MALPRACTICES: This refers to negligence or misconduct

IMPERSONATION: General process of acting on behalf of a client.

IMPERSONATOR: A performed skilled at copying the manner or expression of another mime.

FINGER PRINT: An impression on a surface of the curves formed by the ridges on a finger tip.

BIOMETRICS: Is the use of measurable, biological characteristics such as fingerprints, or iris patterns to identify a person to an electronic system.

ELIMINATION: To get rid of

DESIGN: Is a creative activity whose aim is to establish the multi faceted qualities of objects processes, service and their systems in whole life cycles.

SECURITY ACCESS: Permission granted to users base on their identification.

AUTHENTI CATION: The process of identifying someone base on users name or password in security system

AUTHORIZATION: Act of granting someone the permission to do or take something.

CHAPTER TWO

2.0 LITERATURE REVIEW

Biometrics is the use of measurable, biological characteristics such as finger prints or iris patterns to identify a person to an electronic system. Once these measurements have been taken, they may then be used to authenticate an individual or user. This is done by comparing the sampled biometric against a template taken earlier. This process will be discussed in further detail below. Although biometrics is viewed as an emerging technology, in reality, their use has been documented throughout the history of mankind. In Egypt, thousands of years ago, it was common for individuals to use physical traits or characteristics such as scars, eye and hair color, height, etc., to identify individuals for business transactions. The Old Testament cites the use of a biometric in the Book of Judges 12:5-6. It states: "Then said the men of Gilead unto him, Say now Shibboleth: and he said Sibboleth: for he could not frame to pronounce it right, then they took him and slew him at the passages of Jordan…." The Old Testament. In this example, the pronunciation of the individual was used to identify or authenticate who they were. His repercussions for failing the authentication test were quite a bit more drastic than simply not being granted access, but it was a biometric in use nonetheless.

FINGERPRINT VERIFICATION

Fingerprints have certain natural traits that make them ideal for use in biometric Systems. Fingerprints are developed between the first and second trimester and Remain unchanged (barring any damage or scarring) until death. Fingerprints are Unique. No two people on record have been found to have the same fingerprints. Fingerprint identification has been used by law enforcement agencies for many Years. But this type of one-to-many match is seldom used for commercial Purposes. Most fingerprint systems operate in authentication, rather than Identification, mode. Fingerprint scanning can be done in several different ways. Some systems scan the distinct marks on the finger called minutiae points (similar to the traditionally used police method). Others analyze the distance between ridge endings and ridge burifications on the finger. The positioning of pores and straight pattern matching may also be used. More recent developments include the use of moiré fringe patterns (superimposing of lines and grids to capture three-dimensional surface shape) as well as ultrasound. Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader.

Biometrics is a rapidly evolving technology that has been widely used in forensics, such as criminal identification and prison security, and has the potential to be widely adopted in a very broad range of civilian applications:

- banking security, such as electronic fund transfers, ATM security, check cashing, and credit card transactions;
- physical access control, such as airport access control;
- information system security, such as access to data bases via login privileges;
- government benefits distribution, such as welfare disbursement programs
- customs and immigration, such as the Immigration and Naturalization Service Passenger Accelerated Service System (INSPASS) which permits faster immigration procedures based on hand geometry
- national ID systems, which provide a unique ID to the citizens and integrate different government services
- Voter and driver registration, providing registration facilities for voters and drivers.

Currently, there are mainly nine different biometric techniques that are either widely used or under investigation,

Including face, fingerprint, hand geometry, hand vein, iris, retinal pattern, signature, voice print, and facial thermo grams Although each of these techniques, to a certain extent, satisfies the above requirements and has been used in practical systems or has the potential to become a valid biometric technique , not many of them are acceptable (in a court of law) as indisputable

Evidence of identity. For example, despite the fact that extensive studies have been conducted on automatic face recognition and that a number of face recognition systems are available it has not yet been proven that

- face can be used reliably to establish/verify identity and
- A biometric system that uses only face can achieve acceptable identification accuracy in a practical environment.

Without any other information about the people in it will be extremely difficult for both a human and a face-recognition system to conclude that the different faces shown in are disguised versions of the same person. So far, the only legally acceptable, readily automated, and mature biometric technique is the automatic fingerprint identification technique, which has been used and accepted

In forensics since the early 1970's. Although signatures also are legally acceptable biometrics, they rank a distant second to fingerprints due to issues involved with accuracy, forgery, and behavioral variability. Currently, the world Market for biometric systems is estimated at approximately $112 million. Automatic fingerprint-identification systems intended mainly for forensic applications account for approximately $100 million. The biometric systems intended

For civilian, applications are growing rapidly. For example, by the year 1999, the world market for biometric systems used for physical access control alone is expected to expand to $100 million.

The biometrics community is slow in establishing benchmarks for biometric systems. Although benchmark results on standard data bases in themselves are useful only to a limited extent and may result in excessive tuning of the system parameters to "improve" the system performance,1 they constitute a good starting point for comparison of the gross performance characteristics of the systems. No metric is sufficiently adequate to give a reliable and convincing indication of the identification accuracy of a biometric system. A decision made by a biometric system is either a "genuine individual" type of decision or an

"Impostor" type of decision, which can be represented by two statistical distributions, called genuine distribution and impostor distribution, respectively. For each type of decision, there are two possible decision outcomes, true or false. Therefore, there are a total of four possible outcomes:

1. A genuine individual is accepted,

2. A genuine individual is rejected,

3. An impostor is rejected, and

4. An impostor is accepted.

Outcomes 1) and 3) are correct, whereas 2) and 4) are incorrect. In principle, we can use the false (impostor) acceptance rate (FAR), the false (genuine individual) reject rate (FRR), and the equal error rate (EER) 2 to indicate the identification accuracy of a biometric system. In practice, these performance metrics can only be

estimated from empirical data, and the estimates of the performance are very data dependent. Therefore, they are meaningful only for a specific data base in a specific test environment. For example, the performance of a biometric system claimed by its manufacturer had an FRR of 0.3% and an FAR of 0.1%. An independent test by the Sandia National Laboratory found that the same system had an FRR of 25% with an unknown FAR. To provide a more reliable assessment of a biometric system, some more descriptive performance measures are necessary. Receivers operating curve (ROC) and are the two other commonly used measures. An ROC provides an empirical assessment.

Finger print surface

A fingerprint is the reproduction of a fingerprint epidermis, produced when a finger is pressed against as smooth surface. The most evident structural characteristic of a fingerprint is a pattern of interleaved ridges and valleys; in a fingerprint image.

Ridges (also called ridge lines) are dark where as valleys are bright. Injuries such as superficial burns, abrasions, or cuts do not affect the underlying ridge structure and the original pattern is duplicated in any new skin that grows. Ridges and valleys run in parallel; sometimes they bifurcate and sometimes they terminate. When analyzed at the global level, the fingerprint pattern exhibits one or more regions where the ridge lines assume distinctive shapes (characterized).

Branch and end points of epidermal ridges were used by Sir Francis Galton in 1872 to develop a probabilistic model of fingerprint individuality, and they have been used since then in both forensic (Cummins and Midlo, 1943) and automated matching (Blue, Candela, Gruther, Chellapa, and Wilson, 1994; Hrechak and McHugh, 1990). These Galton features, or minutiae, contain unique information that enables their use in probabilistic analyses. Each Galton feature has a

Specific type, i.e. branch point or end point, a unique location on the fingerprint, and a specific orientation (Stoney and Thornton, 1986). The orientation can be defined for an end point, for example, as the approximate tangent angle to the ridge ending. Most probabilistic models to date have utilized Galton features

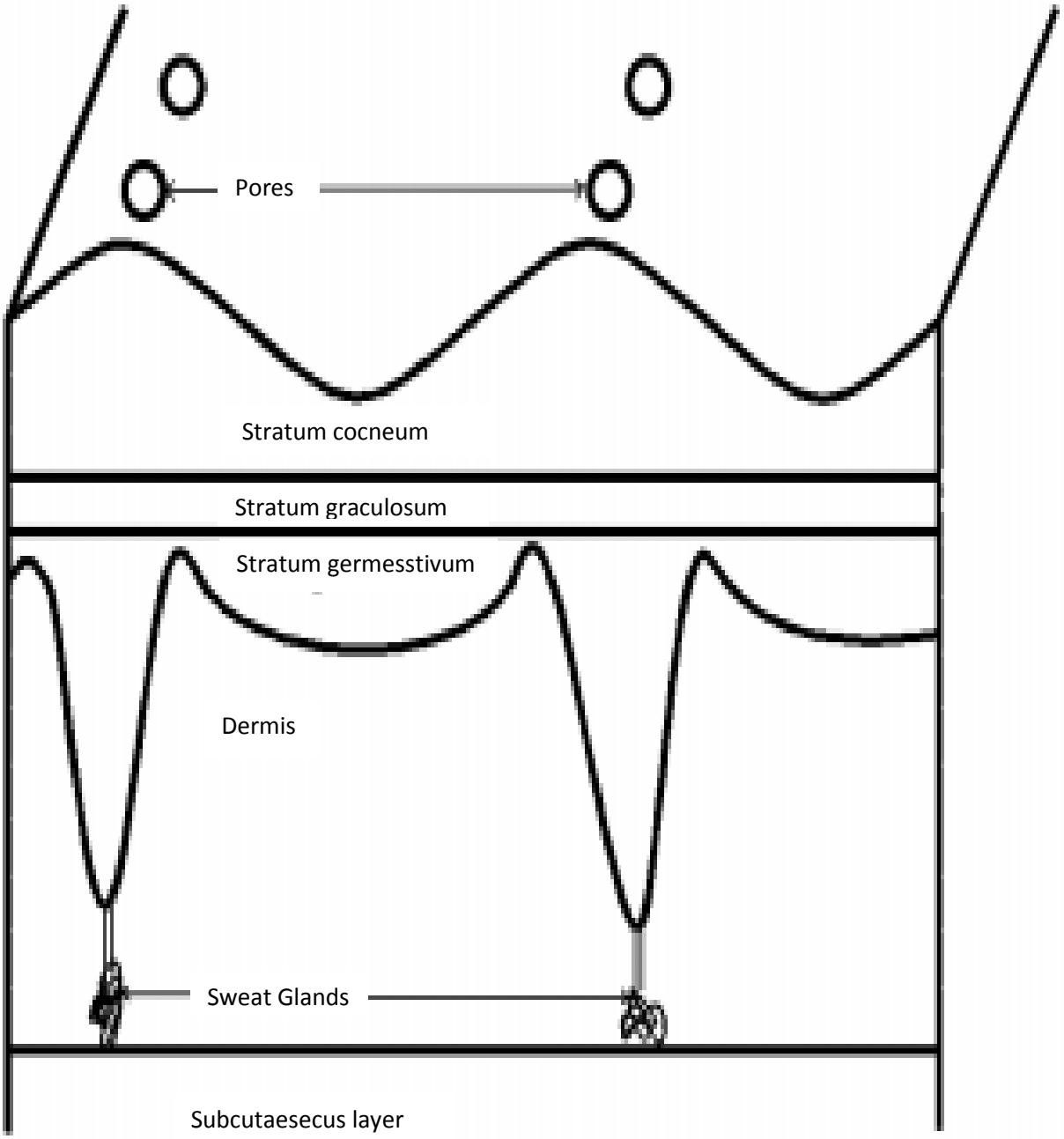
exclusively; two of these models will be presented in this paper. The first model, published in 1977 by James Osterburg, et al at the University of Illinois, determines the probability of occurrence of a certain configuration of Galton features in a fingerprint. Two years later, a member of Osterburg's team, Stanley Sclove, published a paper presenting the occurrence of Galton features as a two-dimensional Markov model. Both of these models can be adapted to use pores instead of Galton features. Pores have been used historically to assist in forensic matching. Although most matching methods have emphasized minutia comparisons and used pores as ancillary comparison features, the ability to match prints based on pore information alone has been documented (Ashbaugh, 1983; Locard, 1912; Stosz and Alyea, 1994). The concept of using pores to match prints has been essentially dormant during the rise of automated fingerprint recognition systems.

PHYSIOLOGY

The uniqueness of a configuration of pores depends on several factors, such as the number of pores involved, their respective shapes and sizes, the locations of these pores with respect to each other, and so on. These factors are all a function of morphology; thus, it would be helpful to discuss briefly the genesis and formation of fingerprints, as well as the implications imposed in the development of pores.

Pores are formed where sweat glands in the subcutaneous layer of the skin generate sweat ducts; these sweat ducts grow through the subcutaneous layer and dermis to the epidermis, where the open duct on the skin's surface presents itself as a pore (Webster, 1992).

According to a 1973 study on skin ridge formation (Hirsch and Schweichel, 1973), sweat glands begin to form in the fifth month of gestation. The sweat gland ducts reach the surface of the epidermis in the sixth month, forming pores.



PHYSIOLOGY OF THE SKIN

The epidermal ridges are not formed until after the sixth month; then, the pattern which has been forming in the glandular fold region is transferred to the epidermis. Hirsch and Schweichel concluded that several forces affect the epidermal pattern

formation; one of these forces is the stabilization that occurs “when sweat gland secretion ducts open on to the surface, at regular intervals, in the papillary ridges.” These openings of the ducts on the surface are the pores, and the regularity of their appearance plays a significant part in the uniqueness of pore configurations.

Once these pores form on the ridge, they are fixed at that location. Considerable research has shown that pores do not disappear, move or spontaneously generate over time (Locard, 1917).

Having look at the certain features of finger print let’s make an analysis on previous research that has made the platform implementation of this technology possible that is the Biometrics.

WHAT IS BIOMETRICS?

Biometrics is the use of measurable, biological characteristics such as fingerprints, or iris patterns to identify a person to an electronic system. Biometrics is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. A physiological biometric would identify by one's voice, DNA, hand print or behavior. Behavioral biometrics are

related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. Some researchers have coined the term behavioral metrics to describe the latter class of biometrics.

More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information.

BIOMETRIC FUNCTIONALITY

Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors. Jain *et al.* (1999) identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. Universality means that every person using a system should possess the trait. Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be

reasonably invariant over time with respect to the specific matching algorithm. Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. Performance relates to the accuracy, speed, and robustness of technology used (see performance section for more details). Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute. No single biometric will meet all the requirements of every possible application.

In verification mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps involved in person verification. In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of verification mode, "where the aim is to prevent multiple people from using same identity".

In Identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be". The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use

some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both). If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area). Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements. We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption

MULTI-BIOMETRIC SYSTEM

Multi-biometric systems use multiple sensors or biometrics to overcome the limitations of un-modal biometric systems. For instance iris recognition systems can be compromised by aging irises and finger scanning systems by worn-out or cut fingerprints. While un-modal biometric systems are limited by the integrity of their identifier, it is unlikely that several un-modal systems will suffer from identical limitations. Multi-biometric obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code). Multi-biometric systems can integrate these un-modal systems sequentially, simultaneously, a combination there of, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. The interested reader is pointed to Cobias for detailed tradeoffs of response time, accuracy, and costs between integration modes.

Broadly, the information fusion is divided into three parts, pre-mapping fusion, midst-mapping fusion, and post-mapping fusion/late fusion. In pre-mapping fusion information can be combined at sensor level or feature level. Sensor-level fusion can be mainly organized in three classes:

1. Single sensor-multiple instances,

2. intra-class multiple sensors, and

3. Inter-class multiple sensors.

Feature-level fusion can be mainly organized in two categories:

1. Intra-class and

2. Inter-class.

Intra-class is again classified into four subcategories:

(a) Same sensor-same features,

(b) Same sensor-different features,

(c) Different sensors-same features, and

(d) Different sensors-different features.

PERFORMANCE

The following are used as performance metrics for biometric systems:

- False accept rate or false match rate (FAR or FMR): the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly

accepted. In case of similarity scale, if the person is imposter in real, but the matching score is higher than the threshold, and then he is treated as genuine that increases the FAR and hence performance also depends upon the selection of threshold value.

- False reject rate or false non-match rate (FRR or FNMR): the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.
- Receiver operating characteristic or relative operating characteristic (ROC): The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be fewer false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).
- Equal error rate or crossover error rate (EER or CER): The rates at which both accept and reject errors are equal. The value of the EER can be easily obtained

from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

- Failure to enroll rate (FTE or FER): the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.
- Failure to capture rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.
- Template capacity: the maximum number of sets of data which can be stored in the system.

HISTORY OF BIOMETRICS

Biometrics has been around since about 29,000 BC when cavemen would sign their drawings with handprints. In 500 BC, Babylonian business transactions were signed in clay tablets with fingerprints. The earliest cataloging of fingerprints dates back to 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina.

ADAPTIVE BIOMETRIC SYSTEMS

Adaptive biometric Systems aim to auto-update the templates or model to the intra-class variation of the operational data. The two-fold advantages of these systems are solving the problem of limited training data and tracking the temporal variations of the input data through adaptation. Recently, adaptive biometrics has received a significant attention from the research community. This research direction is expected to gain momentum because of their key promulgated advantages. First, with an adaptive biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process. Second, it is no longer necessary to re-enroll or retrain the system from the scratch in order to cope up with the changing environment. This convenience can significantly reduce the cost of maintaining a biometric system. Despite these advantages, there are several open issues involved with these systems. For mis-classification error (false acceptance) by the biometric system, cause adaptation using impostor sample. However, continuous research efforts are directed to resolve the open issues associated to the field of adaptive biometrics. More information about adaptive biometric systems can be found in the critical review by Rattani et al.

CURRENT, EMERGING AND FUTURE APPLICATIONS OF BIOMETRICS

Among the different interests, the recent ones include adaptive Multimodal Biometric System, complementary vs. supplementary information, physiological biometrics, spoofing, and so on.

RECENT ADVANCES IN EMERGING BIOMETRICS

In recent times, biometrics based on brain (electroencephalogram) and heart (electrocardiogram) signals have emerged. The research group at University of Wolverhampton lead by Ramaswamy Palaniappan has shown that people have certain distinct brain and heart patterns that are specific for each individual. The advantage of such 'futuristic' technology is that it is more fraud resistant compared to conventional biometrics like fingerprints. However, such technology is generally more cumbersome and still has issues such as lower accuracy and poor reproducibility over time.

John Michael (Mike) McConnell, a former vice admiral in the United States Navy, a former Director of US National Intelligence, and Senior Vice President of Booz Allen Hamilton promoted the development of a future capability to require

biometric authentication to access certain public networks in his Keynote Speech at the 2009 Biometric Consortium Conference.

A basic premise in the above proposal is that the person that has uniquely authenticated themselves using biometrics with the computer is in fact also the agent performing potentially malicious actions from that computer. However, if control of the computer has been subverted, for example in which the computer is part of a botnet controlled by a hacker, then knowledge of the identity of the user at the terminal does not materially improve network security or aid law enforcement activities.

Recently, another approach to biometric security was developed; this method scans the entire body of prospects to guarantee a better identification of this prospect. This method is not globally accepted because it is very complex and prospects are concerned about their privacy. Very few technologists apply it globally.

PRIVACY AND DISCRIMINATION

It is possible that data obtained during biometric enrollment may be used in ways for which the enrolled individual has not consented. For example, biometric security that utilizes an employee's DNA profile could also be used to screen for various genetic diseases or other 'undesirable' traits.

There are three categories of privacy concerns:

1. Unintended functional scope: The authentication goes further than authentication, such as finding a tumor.
2. Unintended application scope: The authentication process correctly identifies the subject when the subject did not wish to be identified.
3. Covert identification: The subject is identified without seeking identification or authentication, i.e. a subject's face is identified in a crowd.

DANGER TO OWNERS OF SECURED ITEMS

When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. If the item is secured with a biometric device, the damage to the owner could be irreversible, and potentially cost more than the secured property. For example, in 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car. In the case of the examination system the impersonator might come with harmful substances so when he is denied access from entering he might decided to use forceful act to gain entrance entreating everybody in the centre to danger.

CANCELABLE BIOMETRICS

One advantage of passwords over biometrics is that they can be re-issued. If a token or a password is lost or stolen, it can be cancelled and replaced by a newer version. This is not naturally available in biometrics. If someone's face is compromised from a database, they cannot cancel or reissue it. Cancelable biometrics is a way in which to incorporate protection and the replacement features into biometrics. It was first proposed by Ratha et al.

Several methods for generating new exclusive biometrics have been proposed. The first fingerprint based cancelable biometric system was designed and developed by Tulyakov et al. essentially, cancelable biometrics perform a distortion of the biometric image or features before matching. The variability in the distortion parameters provides the cancelable nature of the scheme. Some of the proposed techniques operate using their own recognition engines, such as Teoh et al. and Savvides et al., whereas other methods, such as Dabbah et al., take the advantage of the advancement of the well-established biometric research for their recognition front-end to conduct recognition. Although this increases the restrictions on the protection system, it makes the cancellable templates more accessible for available biometric technologies

SOFT BIOMETRICS

Soft biometrics traits are physical, behavioral or adhered human characteristics, which have been derived from the way human beings normally distinguish their peers (e.g. height, gender, hair color). Those attributes have a low discriminating power, thus not capable of identification performance; additionally they are fully available to everyone which makes them privacy-safe.

INTERNATIONAL SHARING OF BIOMETRIC DATA

Many countries, including the United States, are planning to share biometric data with other nations. In testimony before the US House Appropriations Committee, Subcommittee on Homeland Security on "biometric identification" in 2009, Kathleen Kraninger and Robert A Mocny commented on international cooperation and collaboration with respect to biometric data, as follows:

> " *To ensure we can shut down terrorist networks before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Just as we are improving the way we collaborate within the U.S. Government to*

identify and weed out terrorists and other dangerous people, we have the same obligation to work with our partners abroad to prevent terrorists from making any move undetected. Biometrics provides a new way to bring terrorists' true identities to light, stripping them of their greatest advantage—remaining unknown."

According to an article written in 2009 by S. Magnuson in the National Defense Magazine entitled "Defense Department under Pressure to Share Biometric Data" the United States has bi-lateral agreements with other nations aimed at sharing biometric data. To quote that article:

" *Miller [a consultant to the Office of Homeland Defense and America's security affairs] said the United States has bi-lateral agreements to share biometric data with about 25 countries. Every time a foreign leader has visited Washington during the last few years, the State Department has made sure they sign such an agreement."*

Certain members of the civilian community are worried about how biometric data is used. Unfortunately, full disclosure may not be forthcoming to the civilian community. In particular, the Unclassified Report of the Defense Science Board Task Force on Defense Biometrics states in that it is wise to protect, and

sometimes even to disguise, the true and total extent of national capabilities in areas related directly to the conduct of security-related activities. This also potentially applies to Biometrics. It goes on to say that this is a classic feature of intelligence and military operations. In short, the goal is to preserve the security of what the intelligence community calls `sources and methods'.

COUNTRIES APPLYING BIOMETRICS

Countries using biometrics include: Australia, Brazil, Canada, Gambia, Germany, India, Iraq, Israel, Italy, Netherlands, New Zealand, Norway, United Kingdom, and United States.

AUTHENTICATION

An essential aspect of security is the ideology of authentication – the ability to prove that someone or something is what it claims to be. In the systems' security Realm there is three commonly accepted types of user authentication:

1. Something you have – digital certificates, tokens, smart cards and keys

2. Something you know – passwords, personal identification numbers (PIN), or some other piece of personal information such as your pet's Name or mother's maiden name

3. Something you are – a biological trait (a biometric) At first glance, biometrics appears to be the most secure and appealing of the three options. It is nearly

impossible to steal or forge one's genetic traits. It is far more difficult than stealing a password or other personal information such as a PIN. They cannot be lent to another user, and they cannot be forgotten. In most cases, they are not intrusive and are convenient to the end user. But they do pose some interesting challenges as well. For example, if a user's fingerprint pattern is stolen, what can you do? The user can't just simply change their fingerprint like they could a password. A new fingerprint cannot be issued like a certificate could. Recent tests of biometric systems have demonstrated that they are not hack proof. This is interesting food for thought and should be considered when a decision is made to implement any type of authentication system. I will discuss the benefits and concerns in further detail throughout the paper.

HOW DO THEY WORK

THE BIOMETRIC PROCESS

The process model behind a biometric system is generally the same regardless Of the biometric being used. While there will be obvious differences in how Measurements are collected, stored, etc., depending on the biometric chosen or The specific product, the theoretical model remains the same across all types. Following is a brief summary of the processes utilized in most biometrics systems.

COLLECTION AND ENROLLMENT

The first step in any biometric system is collection of the biometric being used. The device used to capture the initial sample will vary depending on the type of physical trait being collected. This could be a reader or sensor used to scan a Fingerprint or palm or a camera to capture facial images or certain aspects of the Retina or iris. In any event, before using the system for the first time for Authentication the user must enroll their biometric sample. This entails the user Presenting a "live" biometric sample of the chosen trait a requisite numbers of Times, usually at least three, so that the system may produce/build a template. In Most cases, this template is then matched with another identifier or reference id, Such as a PIN. Going forward, the user will then enter their PIN, which will tell the system which template to use when comparing against for authentication.

The task of building the template is also sometimes referred to as extraction of the biometric. This is due to the fact that most biometric systems do not store full Images of the biometric in the way that law enforcement agencies store Fingerprints. Rather, certain aspects or points of the biometric are "extracted", and converted into a mathematical code. The attribute extracted depends on The type of biometric you are working with and will be examined more closely when the individual types are reviewed. As noted above, multiple samples of a trait are taken in an attempt to produce the best quality template possible. This will

allow or take into consideration the subtle differences in such things as speech inflection or varying degrees of pressure when a palm or finger is pressed against a reader. It may also include such things as having user's present different facial expressions or using varying degrees of light when taking samples. Collecting a quality sample and building a good template may be the most crucial part of the process. A poor quality template could result in false rejection and require re-enrollment into the system. A stronger template will also help make the system more secure.

TEMPLATE STORAGE

After a user has enrolled in the system and their template has been extracted, that template must be stored so that it may be retrieved later for comparison.

There are three main options for template storage, each with its advantages and disadvantages.

The options are:

1. Store the template at the biometric reading device
2. Store the template remotely in a centralized database
3. Store the template on a portable token (smart card)

The main advantage to storing the templates within the biometric reading device is faster response time. If your templates are stored at the reader you will not

Have to wait on other system or network resources. Most systems can effectively Handle the storage and retrieval of a small amount of templates. But if you have Several thousand users, this may pose a problem. If that is the case, you may be better off storing your templates in a centralized database. Additionally, if Something were to happen to the reader/system you could potentially completely Lose all of your templates. Then re-enrollment of all of your users would be required. Storing your templates in a centralized database makes the most sense if you have many users or multiple systems. It also allows the use of more layers of security to be applied to the process. The main disadvantages would be the Additional resources needed to maintain the additional system and the network Traffic created between the biometric reader and the database. Additionally, if the network were to be down for some reason, the biometric readers would be useless. Storing the template on a smart card has the main advantage that the user will Have sole possession of their trait. They may also then use the card at any number of readers or devices, making it more convenient for the organization to position readers at different locations. Although this storage technique may Make the end user feel more comfortable it may not be in the best interest of the organization. Issuing cards to all users may become cost prohibitive. In addition, It may become more costly if the user were to lose their card and re-enrollment

Plus re-issuing of a card became required. The best storage solution for an organization may be the implementation of multiple storage systems. This will allow the organization to combine the benefits of the solutions and at the same time negate some of the potential disadvantages. Again, the main disadvantage here would be the prohibitive cost.

But for organizations that are able to justify the cost, it would be beneficial to Store the template at both the device level as well as at a central database. The Increased response time could be utilized and the templates would not be lost if There was a failure at either level individually.

COMPARISON AND MATCHING

Each time a user attempts to authenticate against the system, another "live" Biometric sample is taken. Much the same as in the enrollment, the sample is then extracted producing another mathematical code or template. This template Is then compared to the previous template stored in the system. If the specified Requirements for a match are met, the user is authenticated. If the template Taken is not within the successful parameters, the result is a non-match.

Some biometric devices will allow the organization to set the number of attempts allowed for successful authentication. Although you will want to allow reasonable number of attempts in order to let genuine users authenticate, you do not want to allow so many attempts that it may comprise the secure-ness of the system.

Meaning you don't want to give a hacker an exorbitant amount of tries at defeating the system. Additionally, some biometric systems may update the

Stored template each time a live sample is taken. This will help update the template with any changes that may have occurred to the biometric over time.

This could include minor cuts and scrapes, aging, etc. Of course any major

Change to the biometric should result in a non-authentication and re-enrollment may be required.

AUDIT TRAIL

The final step in the biometric process is the storage of the transactional data or audit trail. Audit information can prove to be a very valuable source of Information. It will show you who has successfully authenticated as well has who

Has tried and has been unsuccessful. This may help you pinpoint security problems or issues. You will be able to determine how many attempts at authentications are usually required to successfully authenticate. This can help you fine-tune your system. Again, this information can be stored locally on the device or centrally depending on your preference. Either way, a scheduled review of logs for any unusual discrepancies is always a good security practice.

IDENTIFICATION VS VERIFICATION

Any time you discuss biometrics it is important to make sure that the distinction of Identification vs. Verification is understood. At first glance they may seem like

They are very similar principles, but in actually they are very different. Most biometric devices authenticate users using the verification method. As noted in the process above, during the Collection and Extraction phase, often a PIN is entered so that it may be used to reference the stored template. When a user would attempt to authenticate they would first be required to enter their PIN, which would in turn let the system know which template to retrieve for comparison. The live sample would then be compared against the retrieved template and a match or no-match would result. In this way the system is really just "verifying" that you are who you claim to be. This is often referred to as a one-to-one match.

Identification on the other hand is more detailed and complex. Rather than entering a PIN for reference purposes you just merely present your live sample.

The system then takes the template and compares it to all that it has stored in its database. It keeps checking until it finds a match and is able to declare that it has "identified" you. This is referred to as a one-to-many match. And in some cases it may actually produce many results. Depending on how "strong" the parameters of your system are, it is possible that a live sample may match many stored templates. Although the ability to identify a user is appealing, especially at larger

organizations, this is something that should be considered with caution. In many instances it may not be as secure as a verification model.

COMMONLY USED BIOMETRICS

For the purpose of this paper, I will be subdividing the types of biometrics into two main categories. The first, commonly used biometrics, are those that are Frequently put to use today. The second category, developing biometrics, are up And coming technologies that are either in research stages or just beginning to be utilized for security authentication. It should also be mentioned that just because these are commonly used biometrics does not mean that they are static and immune to change. On the contrary, advancements are being made all the time making them more secure and easier to use.

FINGERPRINT VERIFICATION

Fingerprints have certain natural traits that make them ideal for use in biometric systems. Fingerprints are developed between the first and second trimester and remain unchanged (barring any damage or scarring) until death. Fingerprints are unique. No two people on record have been found to have the same fingerprints. Fingerprint identification has been used by law enforcement agencies for many years. But this type of one-to-many match is seldom used for commercial

purposes. Most fingerprint systems operate in authentication, rather than identification, mode. Fingerprint scanning can be done in several different ways. Some systems scan the distinct marks on the finger called minutiae points (similar to the traditionally used police method). Others analyze the distance between ridge endings and ridge burifications on the finger. The positioning of pores and straight pattern matching may also be used. More recent developments include the use of moiré fringe patterns (superimposing of lines and grids to capture three-dimensional surface shape) as well as ultrasound. Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader.

HAND GEOMETRY

Hand geometry involves the analysis and measuring of the hand and fingers. The user places their hand on the reader with their fingers in designated positions. A camera is then used to capture both a top view, which gives the length and width, as well as a side view, which gives the thickness. Hand geometry is one of the most established uses of biometrics today. It is accurate and fast.

RETINAL SCANNING

Retinal scanning involves using a low intensity light to scan the unique pattern found in the retina portion of the eye. An optical coupler is used to produce the

light, which analyzes the layer of blood vessels found at the back of the eye. It requires the user to position their eye at the reader and focus on a central point.

This is not always convenient for those who wear glasses and some find the idea of a light scanning their eye intrusive, although it is not painful and poses no known danger. Retinal scanning devices are often used in areas where high security is needed and where less consideration is given to convenience and comfort of the user.

IRIS SCANNING

Iris scanning technology is commonly thought of as the most secure or strong biometric system. This is due to the fact that the iris contains a very complex pattern and large number of measurable characteristics that make it practically impossible to replicate. Even a person's right and left iris patterns are different.

For iris scanning, a camera is used to record a digital image of the user's iris.

Contact lenses and glasses do not interfere with the scan. And unlike retinal scanning, there is no intrusive light beamed into the individual's eye. Of all biometric technologies, iris scanning has the most potential for further development.

VOICE VERIFICATION

Voice verification uses a microphone-recording device to capture a sample of a user's voiceprint. Measurements of a number of characteristics are taken, including cadence, pitch, and tone. Voice verification is considered to be a hybrid of physical and behavioral biometric types. On the physical side, the shape of your throat and larynx helps to predetermine your voiceprint. But then again, your experiences help influence such things as inflect and dialect. And although difficult to do, it is possible that one could alter their voiceprint. Additionally, it is important to make sure that the distinction between voice verification and voice recognition is understood. Voice recognition is software that is able to decipher words that are spoken, and is not an authentication technique. Voice verification is fairly simple to implement. Because most workstations come with a microphone of some sort pre-installed, new hardware is usually not needed. It may also be implemented using current telephone systems. Voice verification has run into some opposition and has been accused of being hard to use from an end user perspective. At times it is difficult to enroll in the system as background noises, and static as well as the common cold can cause problems at enrollment and during verification.

SIGNATURE VERIFICATION

Signature verification involves the use of a special pen, tablet, or both to capture the way a person signs their name. Although the final appearance of the signature is important, a number of other attributes are captured as well. These include speed, velocity, pressure, angle of the pen as well as the number of times the pen is lifted from the pad. Signature verification is considered to be very accurate. Additionally, most users will not object to providing their signature for verification, as they are use to identifying themselves by signature all the time (I.e. credit card slips, checks, etc.).

FACIAL RECOGNITION

Facial recognition utilizes distinctive features of the face to authenticate users. A camera of some sort (digital, video or thermal) is used to capture the features. This includes such things as the upper outlines of the eye sockets, the cheekbones, the sides of the mouth, and the location of the nose and eyes.

Video facial recognition maps out a number of points on the face or creates a three-dimensional image to be used for comparison. The user is usually required to stand a few feet away and most systems are capable of compensating for expressions, glasses, hats and beards. Poor lighting can cause problems so most systems will need to be placed in well-lit areas.

Thermal recognition systems use an infrared camera to scan faces and create a digital map of their thermal patterns. This digital image is known as a thermo gram. Branching blood vessels under the skin, which are hotter than the surrounding tissue, are responsible for creating the "hot" spots that the infrared camera picks up. Much like fingerprints, no two people are known to have the same thermo gram.

EXAMPLE OF IMPERSONATION OCCURENCES

Board of Intermediate & Secondary Education (BISE) Lahore's inspection team caught two fake candidates appearing in chemistry paper of the ongoing Secondary School Certificate (Supplementary) Examination 2012. Interestingly, one of the candidates had already done his graduation while the other was caught impersonating for a genuine candidate. Sources in BISE say the candidate who had done graduation might have appeared in the ongoing exam to help some other candidate in solving paper as under the rules such candidates cannot appear in the exam.

This is not for the first time that the BISE examination staff caught fake candidates or impersonators. Each year during examinations, whether of matriculation, intermediate, graduation and even MA/MSc, candidates are caught committing academic crimes like these. However, what can be learnt from such unfortunate but

illegal acts is the growing tendency of negativity and cheating, in the broader sense, among educated youth and the same need to be addressed immediately.

There is no doubt in the fact that no educated youth would put himself or herself into such trouble merely for fun. Obviously, there might be some contributing factors which need to be uncovered and addressed in order to help such individuals to utilize their energies in a positive direction. This is also obvious that an impersonator is academically sound and that's why his/her "services" are "bought" by "poor" students. The possibility of individuals, committing such academic crimes, belonging to economically poor backgrounds is very high since such ventures help make fast bucks. Undoubtedly, unemployment has a role in this tendency as otherwise no sane and educated person would risk his/her future by indulging in such criminal activities. The Punjab government has recently launched Punjab Youth Internship Programme (PYIP) for the unemployed youth, not more than 30 years of age, having acquired 16 years of education. The government aims "to equip the unemployed youth with productive skills to obtain better employment opportunities." The three-month paid internship (Rs 10,000 per month) will allow internees to experience working in public and private organizations. Though the government's critics see PYIP as a politically motivated move ahead of upcoming general elections, there are those who appreciate the initiative and term the same a step in the right direction. Those who oppose the PYIP argue that the government

should strive hard to create employment opportunities instead of engaging educated youth just for a short span of time. Every technology implementation has got a particular fulfillment to achieve the fingerprint biometrics is aimed at granting security access to individuals base on what you are .This technology can be applied to examination system to grant access to only registered individuals. The process of misconduct in the exam which can also include impersonation is called malpractices.

EXAMINATION MALPRACTICE

Examination malpractice is any wrong doing before, during or after any examination. Although one may not be able to rule out examination malpractice in the past, the current trend is alarming and calls for proper management in order to rid the school system of its consequences. Whereas in the past, students tended to hide the acts, now they advertise them with positive blatancy.

The things that others thought right to draw a veil across, the modern biographer reveals with all the gusto of a showman. Ruwa (1997) traced back examination malpractice to 1914. He further reported that in the University of Maiduguri, about 25% of the students interviewed admitted to have engaged in one form of examination malpractice or another. Examination malpractice occurs in both internal and external examinations. In short, it has become an epidemic in the

nation's educational system, which needs a prompt attention. New paragraph the situation of examination malpractice is so embarrassing to the nation that the federal military government in 1984 promulgated Decree 20 to deal with it. Part of the Decree reads thus: Any person who fraudulently or with intent to cheat or secure any unfair advantage to himself or any other person or in abuse of his office, produces, sells or buys or otherwise deals with any question paper intended for the examination of persons at any examination or commits any of the offences specified in section 3(2 7) (c) of this Decree, shall be guilty of an offence and on conviction be sentenced to 21 years imprisonment... (Fagbemi, 1998, p.1 7)

However, Examination Malpractice Act 33 of 1999 revised the above decree but now stipulates punishment ranging from a fine of N50, 000.00 to

N100,000.00 and imprisonment for a term of 3-4 years with or without option of fine. This new development is due to the inability of the appropriate authorities to enforce the old Decree 20 of 1985. Despite all these laws, examination malpractice has been on the increase and this may be due to non implementation of the laws. Reasons for it being the low moral standard in schools, candidates' fear of failure, lack of confidence in themselves, inadequate preparation, laziness and '419' syndrome that have eaten deep into the life of the society. Pratt (1981) stated that students are likely to cheat when they are not prepared for examinations. Ruwa (1997) as well reported that university lecturers are of the opinion that inadequate

teaching and learning facilities, poor conditions of service of teacher's fear of failure by students and admission of unqualified candidates into universities are responsible for examination malpractices.

Fayombo (2004) categorised the reasons for examination malpractices into psychological and sociological causes. The over dependence on certification has led to 'mad ruch' by the populace and the resultant effect is that people either Acquire certificates legimately or otherwise. This messy situation is having a Negative effect on the nation's quality of education and the kind of certificates issued to students at different levels. So many people can no longer defend their certificates.

Okwilagwe (2001) opined that the interest in non-intellectual factors would Seem to have stemmed from the idea that "the human being is a complex whole" That is, man is made up of intellectual, emotional, affective and psychological Traits. For them to develop and reach their full potential in life, these traits must Be understood, harnessed, and be catered for by the school. Students' Involvement examination malpractices have become perennial and institutionalized. It is a testimonial to the flawed process of admission into

Secondary schools and tertiary institutions. It has invariably, reflected in the Multifaceted crises in the nation's educational system. Moral instruction is the detailed information, which concerns the principles of right and wrong behaviors.

The study of moral development has become a lively growth industry within the social sciences. Theories have maintained that human morality springs from emotional disposition that are hardwired into our species. Man is a complete entity, and there is no emphasis on the development of the whole individual that can play out morals. All children are born with a running start on the path to moral development. These children grow up to become adults in society. This is the more reason why children should be trained in self-discipline and filled with useful information. Education expects to provide a full Training for children, and the training involves examination and other forms of assessment from time to time to ascertain the level of knowledge / skill acquisition. This is the more reason why examinations must be well managed. Farrant (1964) states that educationists are often tempted to over-concentrate on certain aspects of the child's make-up to the detriment of the others.

DIMENSIONS OF EXAMINATION MALPRACTICES

Year-in-year-out, students come up with new dimensions of examination malpractices. This is the more reason why drastic steps must be taken. The instances of examination malpractices vary. They range from impersonation, leakage of questions, tampering with results, and computer fraud to fraudulent practices by invigilators, officials and security personnel charged with supervising

examinations. Parents are not left out of the business. Some of these dimensions are discussed below:

1. **Bringing of foreign materials into examination hall**: This is a situation where students bring into the examination hall notes, textbooks, and other prepared materials. The methods are nicknamed as hide and seek microchips, tattoo and magic desk. Sometimes, students bring into the hail unauthorized materials like sophisticated and scientific calculators or four figure tables. Abba (1998) identified some methods like giraffing, contraband, bullet, super print, escort, missiles, pregnant biros and so on.

2. **Assistance from educational stakeholders**: Examination stakeholders include parents, teachers, lecturers, supervisors, security agents, printers and staff of examination bodies. Some parents go to any length in buying question papers for their children while some others even buy certificates for their children. Supervisors colluding with teachers, school principals or students by allowing teachers to come around to teach the students during the examination period; lecturers or teachers releasing question papers or giving underserved marks or allowing students to illegally re-take examination papers. Security agents, printers and staff of examination bodies also sell question papers. Afolabi (1998) stated that: leakage is one problem which appear to defy all solutions. Its persistence,

despite methods of blocking loopholes, is an indication of the malaise and corruption in society

3**. Irregular Activities inside and outside the examination halls**: Students who had the mind to cheat exhibit strange and unwholesome behaviors. They use various such methods as:

(i) Stealing, converting, substituting or misappropriating the scripts of other candidates.

(ii) Substituting worked scripts during or after an examination.

(iii) Tearing part of the question paper or answer booklet during the examination to enhance cheating.

(iv) Seeking and receiving helps from other candidates.

4**. Impersonation**: This a situation where a candidate sits in an examination for Another candidate, thereby pretending to be the real or original candidate.

Impersonation is becoming very rampant, even among school candidates.

Afolabi (1998) listed various methods that have been devised by students and these include:

(a) Posing as a bona-fide candidate: impersonators write the examination on behalf of the candidate they are impersonating. Under-graduates and graduate youth Corpers engage in this type of cheating.

(b) Entry for similar subjects: the plot is hatched right from the entry stage by making the impersonator to enter for the same subjects and sit for the examinations in the hail with the candidate; he writes the candidate's name and number on his booklet while the candidate writes the impersonator's and they exchange scripts before submitting.

(c) Multiple entries: that is candidates entering for the same examination in several parts of the locality. It has also been observed that several candidates struggle unnecessarily for live question papers at the beginning of a paper which are then passed to touts for assistance. Also, candidates deliberately come into the hail with the sole aim of smuggling the question paper out as soon as the paper starts and bringing the solution inside later.

5**. Insult or Assault on Examination Officials**: There are cases of students insulting examination officials as they carry out their businesses. The aim is to distract them from effective supervision, so that they can have a way out.

Sometimes students disturb the conduct of examinations due to poor preparation.

6. **Electronically assisted malpractices**: In recent times, it has been discovered that students make use of electronic gadgets to cheat during examinations. Such things as unauthorized scientific calculators, organizers, compact disc (the smallest size) and mobile phones (GSM) to take advantage of others.

7**. Collusion**: This is a situation where two or more candidates agree to receive or give assistance to each other. If it is verbal, this is called ECOMOG or ECOWAS. Maduabum (1998) identified the use of terms like 'laya', Ecornog, and so on, which are also common among students. Afolabi (1998) said that collusion involves exchange of scripts, passing notes for help from outside and inside the hail; delaying commencement of examination in one centre to obtain question paper from nearby centre which has started, collusion, arising from bribes or threat to the lives and/or property of supervisors.

8. **Mass cheating**: Candidates in an examination hail at times are massively involved in one or some of the irregularities aforementioned.

9**. Inscription:** Students have now advanced to the level of inscribing materials or information on anything like parts of their body, for example palms, thighs, baby pampers; dresses, handkerchiefs, rulers, purses, chairs, tables, walls of examination halls and so on. Some student even code points and synthesize their notes in such a way that they will be the only one that could understand and use them for cheating.

10. **Personality Connection**: There are cases where some influential students make use of godfathers in politics, economic high towers, parents, and cult members to influence the outcome of examinations.

Dangers of Examination Malpractices

Some of the dangers of examination malpractices include:

a. Not being able to defend the certificate (failure in job performance).

b. Perpetual condemnation of the conscience.

c. Possibility of unfulfilled dreams and vision, if the student is rusticated from school or terminated at the working place.

d. Spillover effect borne by parents and other relatives of culprits.

e. The culprit may be initiated into a system of dishonesty and corrupt practices by which they become hardened.

F. it makes nonsense of the educational system and it militates against the country's goal of technological advancement.

g. it discredits certificates issued by national examination bodies and institutions of higher learning and the nation as a whole.

i. It makes students to lose the ability to study or work hard in their studies.

j. When a candidate is caught and expelled, there will be no certificate to show

For whatever year(s) they might have put into their educational career.

But this research focus on the elimination of exam impersonation which is a current form exam malpractice using finger print biometrics. all methodology analysis of design and method of data collection would be evaluated in chapters ahead of this project.

CHAPTER THREE

3.0 METHODOLOGY AND ANALYSIS OF THE PRESENT SYSTEM

3.1 THE RESEARCH METHODOLOGY

METHODOLOGY

This proposed examination impersonation elimination system uses fingerprint identification. In identification, the system recognizes an individual by comparing his/her biometrics with every record in the database. In general, biometric identification consists of two stages:

i. Enrollment and

ii. Authentication

During enrollment, the biometrics of the user is captured (using a fingerprint reader, which are likely to be an optical, solid state or an ultrasound sensor or other suitable device) and the unique features are extracted and stored in a 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 enrollment process is carried out by an administrator in the examination system.

During authentication, the biometrics of the user is captured again and the extracted features are compared (using a matching algorithm) with the ones already existing in the database to determine a match. The identification accuracy of a biometric system is measured with the false (impostor) acceptance rate (FAR) and the false (genuine individual) reject rate (FRR). The FAR/FRR ratios depend, among other factors, on the type of difficulty of the algorithms used in the fingerprint extraction. Usually, algorithms with high-medium complexity lead to acceptable low FRR/FAR. However, as it becomes more complex the computational cost increases which leads to undesirable high processing times. Thus, the overall performance of the identification system should be evaluated in terms of FAR/FRR, computational cost and other factors such as security, size and cost.

It has been established that physical achieves are not always helpful a much better alternative is to use biometrics concept that can facilitate stronger security to the problem of exam impersonation.

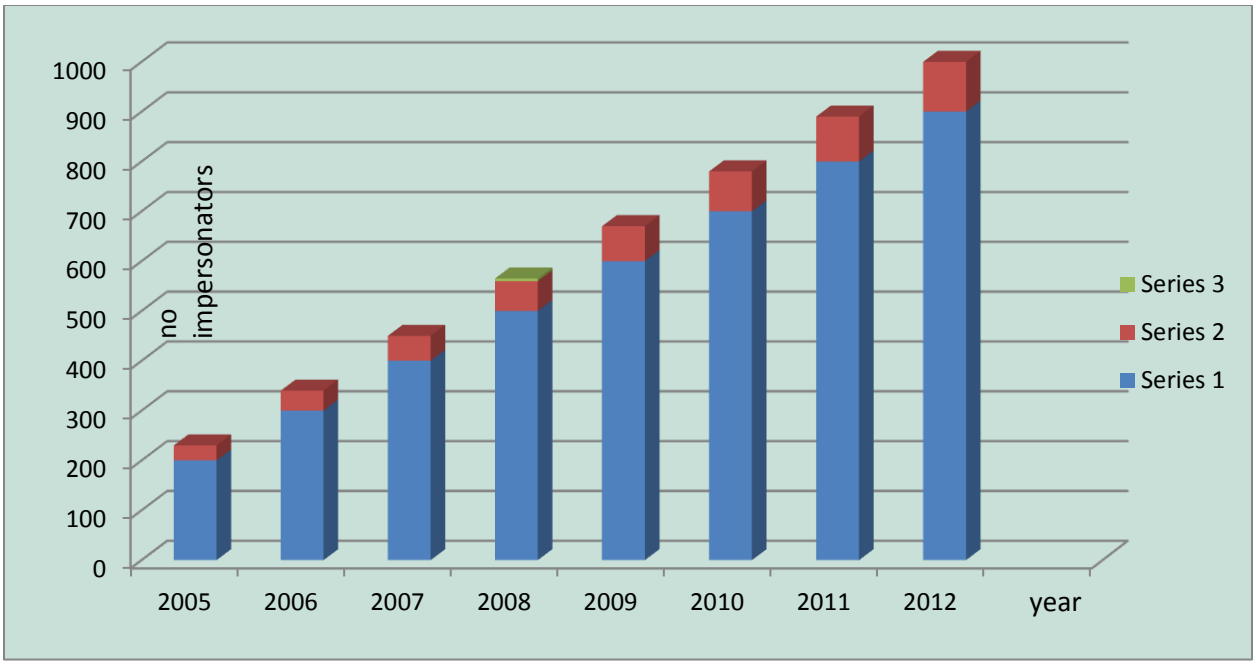
This implies the creation of database management system (DBMS) which ensure that computer records are kept up to date and made available on demand to those who need them for planning and operational purpose. The level of success achieved in caring out this research work is owed to the methodology adopted.

A research methodology is a systematical programming approach of a well defined procedure that should be followed in caring out a thorough research work .an adequately suitable methodology would ensure a very detail research work and ensure a higher degree of accuracy and efficiency is adopted.

In other to attain quiet a reasonable acceptance of the research work we made use of the internationally accepted software engineering model, which is **STRUTURED SYSTEM ANALYSIS AND DESIGN METHODOLOGY (SSADM).**

The (SSADM) is a system approach` to the analysis and design of information system. It involves the application of a sequence of analysis, documentation and design tasks concern with the analysis of the current system logical data design, logical process design, etc. The research methodology used helps us to ensure that a thorough study of the present system is effectively carried out thus helping the project research team to completely understand the modus operandi of the present system and its irregularities which have made it fall in standard so as to know how the new system should be structured and the functionalities needed in it to address the seemingly existing problems discovered. This helps to know if there should be total overhauling of the existing system or if only modification should be made.

Graph describing the usage of the current system (2005-2012) -



This graph simply describe that there is an increase in the number of impersonators yearly and at an average of plus 100 persons every year this have brought about a fall in standard of education and increase in exam malpractice.

METHOD OF DATA COLLECTION

While using the SYSTEM STRUCTURED ANALYSIS AND DESIGN METHOLOGY the following sequence of step where carried out and they include.

FEASIBILITY STUDY

An in-depth study was carried out to determine the possibility of implementing an management information system for the project. This investigation is essential to

building an information system that keeps record of all the student personal identity in the university, college of education, polytechnic secondary schools. Etc. Under this study the following techniques where found beneficiary in the course of gathering relevant fact and details for this project work.

- **OBSERVATION METHOD**

Due to the importance attached to collection of accurate information from the right, authentic and reliable source. It is embarked on the mode of carrying out activities and project implementation in the university examination system. This method was adopted for the following reasons.

To have a firsthand knowledge about the method of exam in the school the system for entrance into the exams and avoid exaggeration.

To allow organization see the whole detail needed for the new system and its structure.

- **STUDYING OF PROCEDURAL MANUALS**

Written document about the university and the procedure manuals seen showed the different portfolios obtainable in the project each with its designated functions obtainable in the project .this method of data collection was very useful in that it served as an eye-opener for asking reliable questions pertaining to the activities of the project.

- **INTERVIEWING METHOD**

Interviewing is another sophisticate means of collecting data this method involves face to face interpersonal role situation in which questioned are raised and answer are supplied. In this method of data collection we analyze why the previous systems have refused to solve the problem faced and the effect of its persistence occurrence in the society.

In view to investigation, MR Okeke the public administration departmental HOD and the head of exams and record was interviewed .I received useful answer during my time of interviewing him which also provided certain analysis of the proposed system during my time of interviewing him information such as

- How the act of examination impersonation is carried out.
- The reason why student indulge in exams impersonation.
- The mode of registration for the exam.

3.3 EVALUATION AND INSPECTION OF DOCUMENTS

Close examination of some document was carried out and it proved to be an important method, in the course of the investigation through the inspection some deductions and inference which are of immense benefit to this research were drawn. Example of document that was inspect was the student examination brochure, student examination course to know the number of courses, document

from the internet relevant to institution their credit unit and their course code each level offers.

3.4 ANALYSIS OF THE CURRENT SYSTEM

The current systems do not make use of any biometrics concept. In the W.A.E.C examination system student will first of all register their course which they will take in the exam and after the registration process an e-photo card or an ID card is brought to the exam hall, after the registration student passport is also registered but this still not a strong measure or security because the eyes is what is used in this case to check for the occurred passport and the physically occurring human. Certain student who is not capable of writing the proposed course due to laziness in studies might pay people to come and write the courses for him. The persons involve is the impersonator and tend to be committing an exam malpractices. When it's time of exams student are expected to arrive at the examination hall with their photo card or id card this id card or photo card serve as an authorization for them to gain access to the exam hall and participate fully in the exam. Since the process use is what you have and not what you are impersonator can simply make black and white photocopy of the photo card making his picture to be dark so when check during the exam since the picture is not clear enough they would be able to accuse them of writing exams for someone that's is if they where notice. Also in the university system not all student are know by the lecturers student simply

arrive the exam hall for the exam and enters with his id card and course form without been check properly if he is a student of the institution as a result student from other school can come and impersonate for other student been the fact that he was going to be paid certain amount of money this is now common among youth and graduating student since there is proper security check for the student to ascertain if truly they are main to write the course and if the from that institutions. Using the eye a physical matching is now take between the passport that has been printed and the physically present human to check if the student that has register is actually the one writing the exam and if not he/she is apprehend. But this has proven to be very inefficient with a significance test if 0.0001 confidence interval this method has proven to be inappropriate.

3.4 PROBLEMS OF THE EXISTING SYSTEM

Several problems tend to exist within the use of the system and as such include:

- Inefficient in its usage and comprehend the act of exam impersonation
- It deals with the process of authorization. This is a concept of "what you have" which can be manipulated at anytime.
- Matching to establish security measures occurs through the physical eye and this is a very big problem and requires great power of recognition, hence an impersonator can be present with recognition.

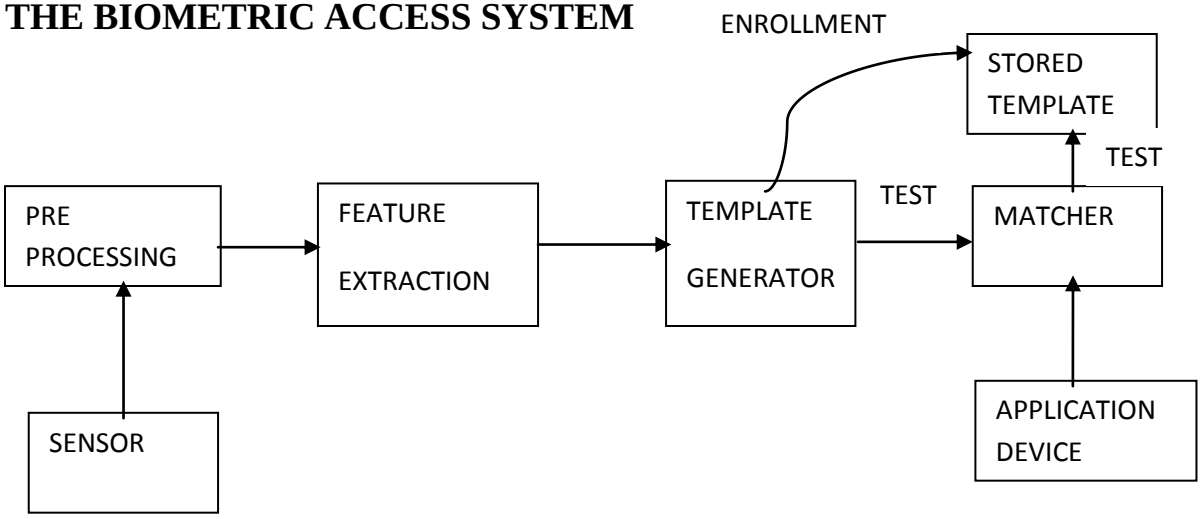
CHAPTER FOUR

4.0 SYSTEM SPECIFICATION AND DESIGN

During the software development many stages are involved that ensure the successful development of the desired software. The design stage which determines how the software product will meet its requirement and implementation which creates the software product as designed before the testing stage that ensures that the software product meets user's requirement.

System design and implementation, specification is very important in every software development at this stage every factor are put into consideration by the developer while making his design the system should be design in such a way that there is a correlation between inputs and output also the format for design should be made in a way that it will be acceptable and interacting to end users.

THE BIOMETRIC ACCESS SYSTEM



The diagram above shows a simple block diagram of a biometric system.

The main operations the system can perform are enrollment and test. During the enrollment, biometric information from an individual is stored. During the test, biometric information is detected and compared with the stored information. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust.

The first block (sensor) is the interface between the real world and our system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. For the sake of our discussion the sensor may be a fingerprint capture device which provides an interface where the user thumbs print. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise or image), to use some kind of normalization, etc. The above feature is built into the capture device.

In the third block features needed are extracted. This step is an important step as the correct features need to be extracted and the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of all the characteristics extracted from the source, in the optimal size to allow for adequate identification. If enrollment is being performed the template is simply stored somewhere (on a card or within a database or both). If a matching

phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).

SYSTEM OVERVIEW

The proposed system provides solution to exam impersonation problems through the use of interacting software that is interfaced to a fingerprint device. The student bio-data (Matriculation number, Name, Gender and Date of Birth) and the fingerprint are enrolled first into the database. The fingerprint is captured using a fingerprint device.

For examination, the student places his/ her finger over the fingerprint device and the student's matriculation number is sent to the database as having attended taking that particular exams. During the exam the school management is expected to come with system containing the students' database of information for that exams and each student is expected to thumb print before entering for the exams during the process of thumb printing if a student that has not registered for the exams and he wants to write the exam a matching template will fail as the student will be apprehended as impersonator.

SYSTEM DESIGN

The development of the prototype was designed using the micro-soft visual studio and micro soft access as the database.

An elimination of exam impersonator using finger print biometrics is a highly specialized system that records students' attendance by comparing a single fingerprint image with the fingerprint images previously stored in a database during the registration process. The exam impersonator elimination system is the principle behind the AFAS.

The major factors in designing an examination impersonator elimination system: choosing the hardware and software components and integrating both to work together, defining the system working mode (verification or identification), dealing with poor quality images and other programming language exception, and defining administration and optimization policy.

Exam impersonator elimination system framework is divided into three parts: Hardware design, Software design, finger print approach and Report Generation. Each of these is explained

HARDWARE ARCHITECTURE

The hardware to be used can be divided into two categories – fingerprint scanner which captures the image and a personal computer which: houses the database, runs the comparison algorithm and simulates the application function. The

fingerprint scanner is connected to the computer via its USB interface. Basically this work does not involve the development of hardware. Using the Secugen Fingerprint Reader, the GrFinger Software Development Kit (SDK) toolbox provided by the Griaule (will explain the detail) can be used as an interface between the fingerprint reader and the impersonation software.

Hardware is the physical component that makes up the computer system. It refers to the physical interface of the component that can be felt, seen and touched .every software require some prerequisite for the software to operate normally.

The following are the hard ware requirement:

HARDWARE REQUIREMENT:

Processor Pentium IV

Hard disk capacity of 90 GB and above

Ram capacity of 512mb and above

Processor speed of 1.8 GHz and above

Flash drive

Keyboard enhanced

Mouse

Monitor14 inch svga

GrFinger Software Development Kit (SDK)

Fingerprint Reader.

FINGER PRINT DEVICE

SOFTWARE REQUIREMENT

Let’s define what software is and its related component

Computer software, or just software, is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it. Software refers to one or more computer programs and data held in the storage of the computer. In other words, software is a set of programs, procedures, algorithms and its documentation concerned with the operation of a data processing system. Program software performs the function of the program it

implements, either by directly providing instructions to the computer hardware or by serving as input to another piece of software. The term was coined to contrast to the old term hardware (meaning physical devices). In contrast to hardware, software "cannot be touched". Software is also sometimes used in a more narrow sense, meaning application software only. Sometimes the term includes data that has not traditionally been associated with computers, such as film, tapes, and records.

Computer software is so called to distinguish it from computer hardware, which encompasses the physical interconnections and devices required to store and execute (or run) the software. At the lowest level, executable code consists of machine language instructions specific to an individual processor. A machine language consists of groups of binary values signifying processor instructions that change the state of the computer from its preceding state. Programs are an ordered sequence of instructions for changing the state of the computer in a particular sequence. It is usually written in high-level programming languages that are easier and more efficient for humans to use (closer to natural language) than machine language. High-level languages are compiled or interpreted into machine language object code. Software may also be written in an assembly language, essentially, a mnemonic representation of a machine language using a natural language alphabet. Assembly language must be assembled into object code via an assembler. Every

software can be divided into system software or application software. But they are both necessary to form a computer system.

APPLICATION SOFTWARE

Application software, also known as an application or an app, is computer software designed to help the user to perform specific tasks. Examples include enterprise software, accounting software, office suites, graphics software and media players. Many application programs deal principally with documents. Apps may be bundled with the computer and its system software, or may be published separately. In recent years, the abbreviation "app" has specifically come to mean application software written for mobile devices, with the abbreviation in particular representing both the smaller size and smaller scope of the software (i.e. an app whose sole purpose is to display an image representation of the current weather).

Application software is contrasted with system software and middleware, which manage and integrate a computer's capabilities, but typically do not directly apply in the performance of tasks that benefit the user. The system software serves the application, which in turn serves the user. Similar relationships apply in other fields. For example, a shopping mall does not provide the merchandise a shopper is seeking, but provides space and services for retailers that serve the shopper. A bridge may similarly support rail tracks which support trains, allowing the trains to

transport passengers. Application software applies the power of a particular computing platform or system software to a particular purpose. Some applications are available in versions for several different platforms; others have narrower requirements and are thus called, for example, a Geography application for Windows or an Android application for education or Linux gaming. Sometimes a new and popular application arises which only runs on one platform, increasing the desirability of that platform. This is called a killer application.

SYSTEM SOFTWARE

System software is a program that manages and supports the computer resources and operations of a computer system while it executes various tasks such as processing data and information, controlling hardware components, and allowing users to use application software. That is, systems software functions as a bridge between computer system hardware and the application software. System software is made up of many control programs, including the operating system, communications software and database manager. There are many kinds of computers these days. Some of them are easier to learn than others. Some of them perform better than others. These differences may come from different systems software.

THREE KINDS OF PROGRAMS

Systems software consists of three kinds of programs. The system management programs, system support programs, and system development programs are they. These are explained briefly.

SYSTEM MANAGEMENT PROGRAMS

These are programs that manage the application software, computer hardware, and data resources of the computer system. These programs include operating systems, operating environment programs, database management programs, and telecommunications monitor programs. Among these, the most important system management programs are operating systems. The operating systems are needed to study more details. There are two reasons. First, users need to know their functions first. For the second, there are many kinds of operating systems available today.

Telecommunications monitor programs are additions of the operating systems of microcomputers. These programs provide the extra logic for the computer system to control a class of communications devices.

SYSTEM SUPPORT PROGRAMS

These are the programs that help the operations and management of a computer system. They provide a variety of support services to let the computer hardware

and other system programs run efficiently. The major system support programs are system utility programs, system performance monitor programs, and system security monitor programs (virus checking programs).

SYSTEM DEVELOPMENT PROGRAMS

These are programs that help users develop information system programs and prepare user programs for computer processing. These programs may analyze and design systems and program itself. The main system development programs are programming language translators, programming environment programs, computer-aided software engineering packages A software requirements specification (SRS) — a requirements specification for a software system — is a complete description of the behavior of a system to be developed and may include a set of use cases that describe interactions the users will have with the software. In addition it also contains non-functional requirements. Non-functional requirements impose constraints on the design or implementation (such as performance engineering requirements, quality standards, or design constraints).

The software requirements specification document enlists all necessary requirements for project development. To derive the requirements we need to have clear and thorough understanding of the products to be developed. This is prepared after detailed communications with project team and the customer.

SOFTWARE ARCHITECTURE

The software architecture consists of: the database and the application program.

Database: The database consists of tables that stores records implemented in Microsoft access database and sql statement. However, this can be migrated to any other relational database of choice. Microsoft access is fast and easy, it can store a very large record and requires little configuration.

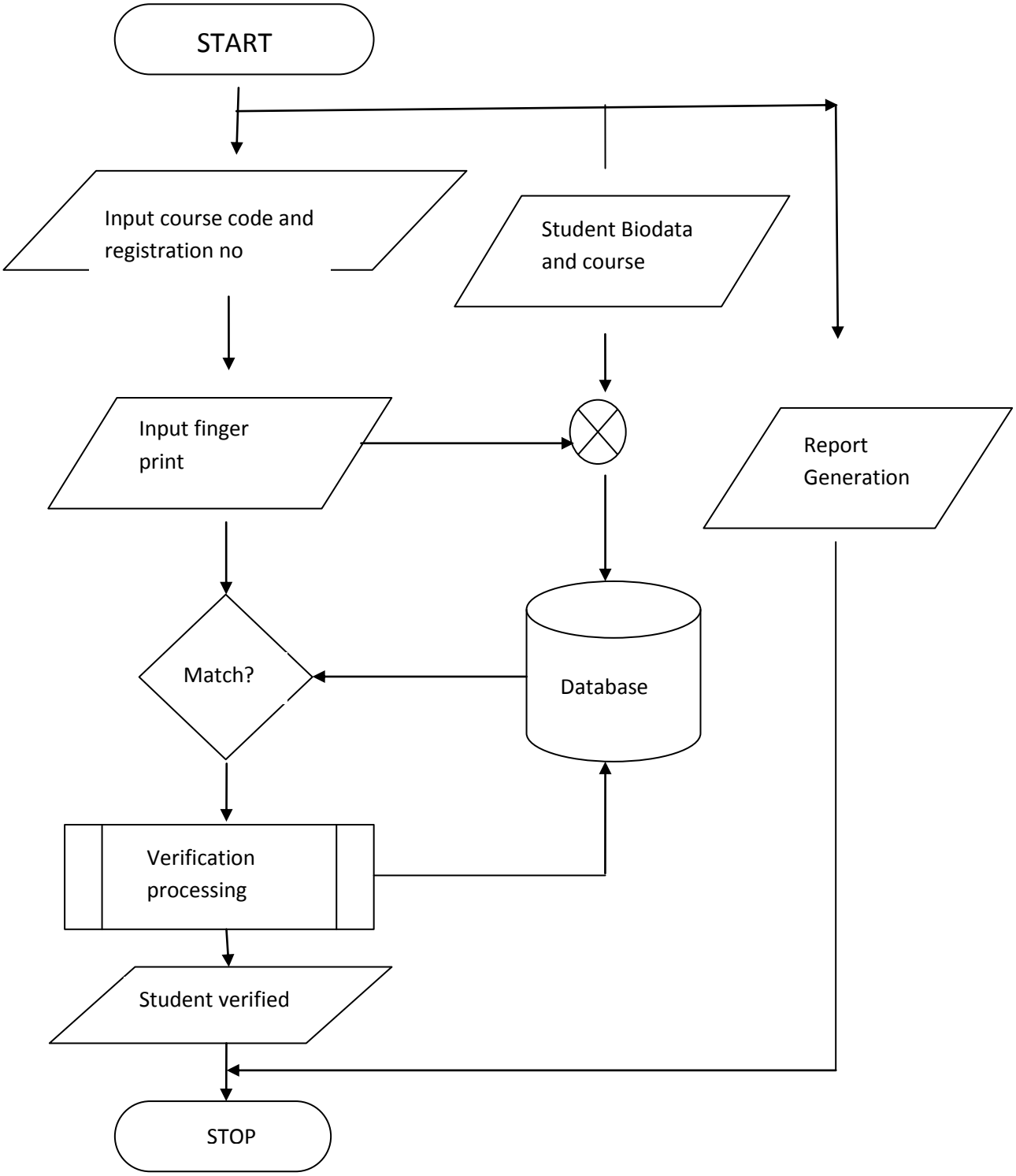
Application Program: The application program is developed with Microsoft vb.net programming language using Microsoft Visual Studio framework and it provides a user interface for the elimination of the exam impersonation. The advantages of Microsoft vb.net programming language are its robustness, easy to program, has an excellent database connectivity, runs on the two most common operating system platforms (Windows and Unix) and it has a larger user community that provides online support.

SOFTWARE REQUIREMENT

MICRO-SOFT ACCESS

VIUAL STUDIO PLATFORM

THE PROGRAM FLOW CHART



LOGIN INPUT TABLE

S/N	FIELD NAME	CHARACTER SIZE	OBJECT TYPE	OBJECT INPUT METHOD	CHARACTER TYPE
1	USERSNAME	40	TEXTBOX	TYPE	CHAR
2	PASSWORD	40	TEXTBOX	TYPE	CHAR

OUT PUT LOGIN FORM

S/N	OBJECT TYPE	STATUS
1	MSGBOX	SHOW
2	FORM3	VISIBLE

INPUT TO THE REGISTRATION SYSTEM

S/N	FIELD NAME	DATA TYPE	FIELD VARIABLE	CHARACTER SIZE	OBJECT TYPE
1	STUDENT NAME	CHAR	SN	100	TEXTBOX
2	REGISTRATIO NO	CHAR	RN	16	TEXTBOX
3	ADDRESS	CHAR	AD	1000	TXTBOX
4	GENDER	CHAR	GN	18	COMBOBOX
5	DEPARTMENT	CHAR	DP	100	COMBOBOX
6	LEVEL	CHAR	LV	8	COMBOBOX
7	STATE OF ORIGIN	CHAR	ST	500	COMBOBOX
8	EXAMINATIO N CENTER	CHAR	EC	500	COMBOBOX
9	BIOMETRICS IDNO	INT	BI	9	LABEL

10	FINGERPRINT TEMPLATE	STRING	FT	NULL	TEMPLATE
11	PASSPORT PHOTO GRAPH	STRING	PH	NULL	PICTUREBOX

EXAMPLE OFF INPUT

S/N	FIELD NAME	DATA TYPE	CHARACTER SIZE	OBJECT INPUT METHOD
1	STUDENT NAME	FRANKLYN IHESIULO	17	INPUT
2	REGISTRATION NO	CST/2008/219	12	INPUT
3	ADDRESS	5 YAYA CLOSE CASCO FESTAC TOWN LAGOS	36	INPUT

4	GENDER	MALE	4	SELECTION
5	DEPARTMENT	COMPUTER SCIENCE	16	SELECTION
6	LEVEL	400L	4	SELECTION
7	STATE OF ORIGIN	IMO	3	SELECTION
8	EXAMINATION CENTER	CENTER 1	8	SELECTION
9	BIOMETRICS IDNO	171	3	AUTO INPUT
10	FINGERPRINT TEMPLATE	STRING	6	THUMB PRINT
11	PASSPORT PHOTOGRAPH	STRING	6	FOLDER SELECTION

OUTPUT TABLE VERIFICATIO SYSTEM

S/N	FIELD NAME	OUTPUT VALUE	STATUS
1	STUDENT NAME	IHESULO FRANKLYN	OK
2	REGISTRATION NO	CST/2008/219	OK
3	BIOMETRICS ID NO	171	OK
4	FINGERPRINT TEMPLATE	THUMB TEMPLATE	VERIFIED
5	PASSPORT PHOTO GRAPH	PASSPORT	VERIFIED

CHAPTER FIVE

CONCLUSION, RECOMMENDATION

5.0 CONCLUSION

In this paper we designed 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. Future work may see to the implementation of the proposed model in Examination Halls Apart from the fact that it takes us to another level in human machine interface, it is economical and easy to use, it should be adopted by Educational institutions in Nigeria.

5.1 RECOMMENDATION

The fingerprint biometric is as good as it is, in improving security, has some challenges which require further work. The first of these challenges is spoofing i.e. the use of forged biometric object (e.g. Plastic finger) in accessing a secured system. An example of such is described in an article published by a group from

Yokohama National University in Japan. In this article Matsumoto and colleagues developed a method to spoof fingerprint devices (T Matsumoto et al, 2002) by making a mold from plastic, originating from both a live finger and a latent fingerprint. Artificial fingers were then created from the casts using gelatin, commonly used for confectionary, where the resultant casts were termed "gummy fingers". The resultant artificial finger works perfectly like the original natural finger in identifying the user. This development poses a serious challenge to the future of biometrics. However, a readymade solution to this problem is liveness detection. The goal of liveness testing is to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture. Another challenge is the security of the biometric template. Once this is compromised the user loses his identity for life. A compromised PIN can be changed to remove security threat but this is not the same for biometric template because of its permanence. The recommendation is that more works need to be done in evolving a more robust liveness detection algorithm that eliminate the danger of spoofing and guarantee a true identification of the user.

REFERENCES

.Awanb or, D. (2005). "Credentialing process in the Nigerian educational

2005. and Users Identity in Automatic Teller Machine, International Journal

Artificial 'Gummy' Fingers on Fingerprint Systems", Proceedings of SPIE,

By the House of Representatives Committee on Education Held at the

Cognitive Informatics and Natural Intelligence, 2(2), 95

Commission of the European Communities (1993) "Glossary of Information

Control in Automatic Teller Machine UsingDenotational Mathematics

Delivered in a Two Day Summit on Examination Malpractice in Nigeria Organized

Faculty of Education, Ambrose Alli University, Ekpoma, November 10-12,

In Proceedings of the Sixth International Conference on Cognitive

Informatics (ICCI'07) (pp. 284-293). Lake Tahoe, CA: IEEE CS Press. Wang, Y.

(2008a). Deductive semantics of RTPA. The International Journal of

information systems security,.

International Journal of Computer Science and Network Security, Vol. 11,

L Thalheim, J Krissler, (November 2002)."Body Check: Biometric Access

magazine. No. 11, ISSN 1738 of Physical Science, Vol 2, No. Protection

Devices and their Programs Put to the Test", c't

Rufai M. M., Adetoba B. T., Adigun J. O. (2007). Biometric Access

Rufai M. M., Adigun J. O., Yekini N. A. (2007). Modelling Discretional Access

Shehu Musa Yar' Adua Centre, Abuja, August 15-16, 2006

system". Keynote Address Presented at the First Annual Conference of the

Systems Security "Contract 52001, Definitions within

T Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, (January, 2002). "Impact of

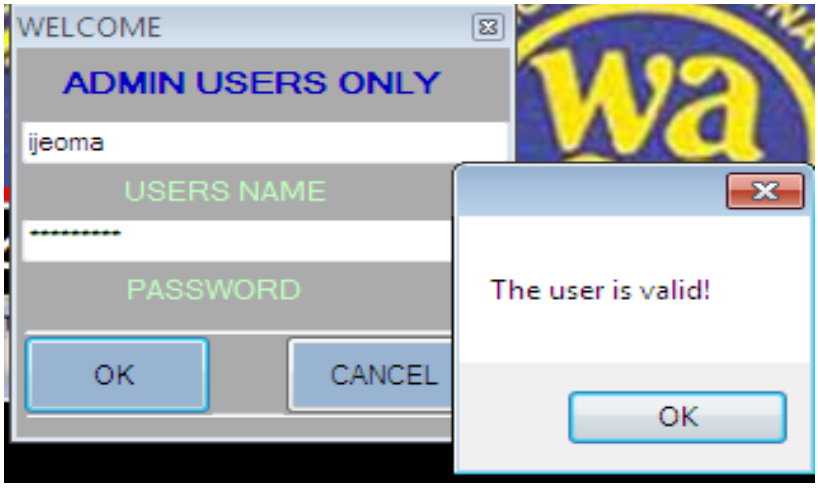
vol. 4677.

Wang, Y. (2007a). Formal description of the cognitive process of memorization.

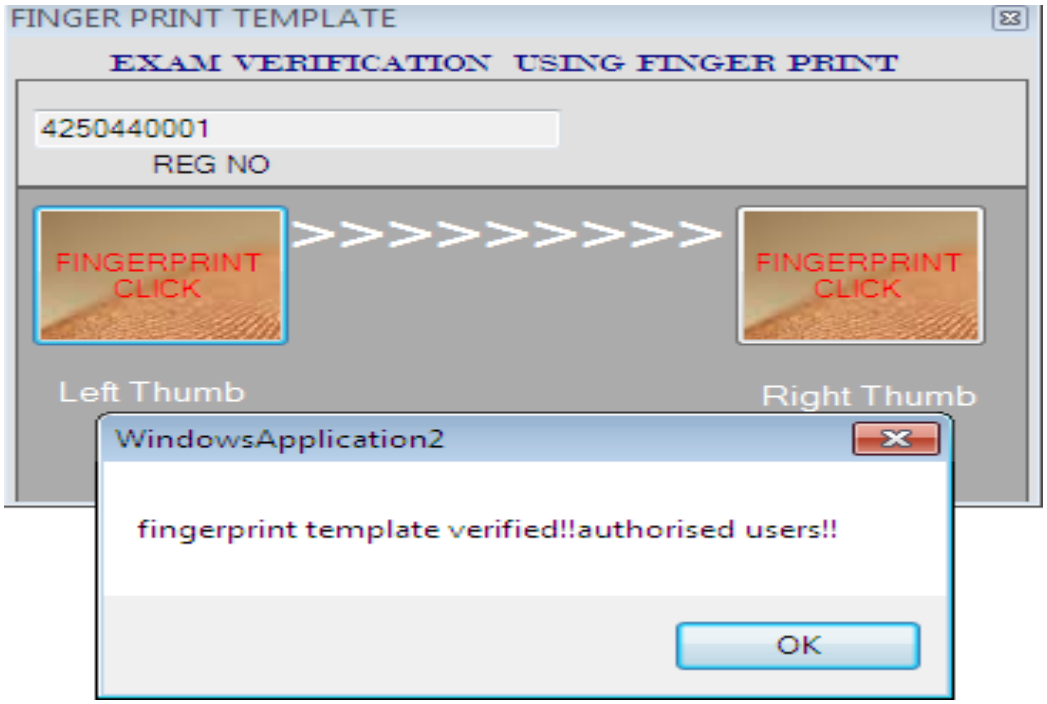
APPENDIX A

WELCOME FORM

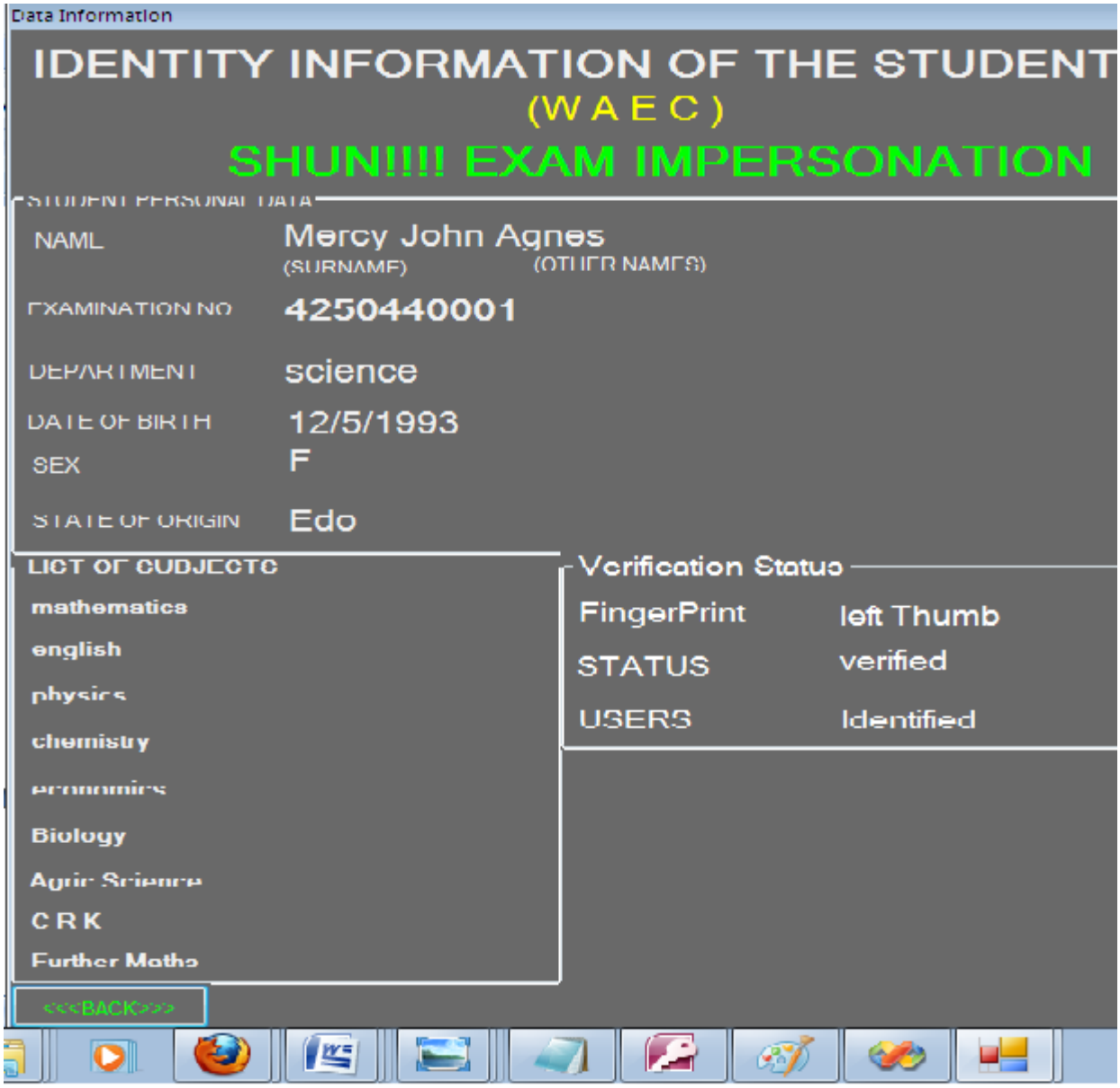
ADMIN AUTHENTICATION



AUTHENTICATION PROCESS



DATA DISPLAY FORM



APPENDIX B (PROGRAM CODES)

```
Public Class Form6

    Private Sub Form6_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load

        Timer1.Enabled = True

        Label2.Text = "SAY NO TO EXAM
MALPRATICE""IMPERSONATION!!!"

    End Sub


    Private Sub Timer1_Tick(ByVal sender As System.Object, ByVal e As
System.EventArgs)


    End Sub


    Private Sub Timer1_Tick_1(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Timer1.Tick

        If Label2.Visible = True Then

            Label2.Visible = False

        Else

            Label2.Visible = True

        End If
```

```
If ProgressBar1.Value < ProgressBar1.Maximum Then
    ProgressBar1.Value += 1
    If ProgressBar1.Value = 10 Then


    ElseIf ProgressBar1.Value = 20 Then


    ElseIf ProgressBar1.Value = 30 Then


    ElseIf ProgressBar1.Value = 40 Then


    ElseIf ProgressBar1.Value = 50 Then


    ElseIf ProgressBar1.Value = 60 Then


    ElseIf ProgressBar1.Value = 90 Then
        Label3.Text = "WELCOME....."


    ElseIf ProgressBar1.Value = 100 Then
```

```
            Form1.Show()
            Me.Hide()
        End If


Imports System.IO
Imports System.Data
Imports System.Data.OleDb
Public Class Form5


    Private Sub Form5_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load


    End Sub


    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button1.Click
        Dim con As OleDbConnection = New
OleDbConnection("Provider=Microsoft.ACE.OLEDB.12.0;Data
Source=c:\Users\user\Documents\ijeoma.accdb;Persist Security Info=False;")
```

```
        Dim cmd As OleDbCommand = New OleDbCommand("SELECT * FROM
ijeoma WHERE password = '" & TextBox1.Text & "' ", con)
        con.Open()
        Dim sdr As OleDbDataReader = cmd.ExecuteReader()
        ' If the record can be queried, Pass verification and open another form.
        If (sdr.Read() = True) Then
            MessageBox.Show("WELCOME!")
            Form3.Show()
            Me.Hide()
        Else
            MessageBox.Show("Invalid Adminpassword!")
        End If
    End Sub

    Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button2.Click
        TextBox1.Text = ""
Imports System.Data.OleDb
Imports System.Data
Public Class Form
```

```
    Dim query As String
    Dim con As OleDbConnection
    Dim comm As OleDbCommand
    Dim rdr As OleDbDataReader
    Dim da As OleDbDataAdapter
    Dim i As Integer = 0
    Dim bind As New BindingSource
    Dim ds As New DataSet
    Dim counter As Integer = 1
    Private Function reader(ByVal sql As String) As OleDbDataReader
        comm = New OleDbCommand(sql, con)
        reader = comm.ExecuteReader
    End Function
    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button1.Click
        Form2.Visible = True
        Me.Hide()
    End Sub
```

```
    Private Sub DataGridView1_CellContentClick(ByVal sender As System.Object,
ByVal e As System.Windows.Forms.DataGridViewCellEventArgs) Handles
DataGridView1.CellContentClick


    End Sub


    Private Sub Form3_Load(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles MyBase.Load

        Dim ConnStr As String = ("Provider=Microsoft.ACE.OLEDB.12.0;Data
Source=c:\Users\user\Documents\ijeoma2.accdb;Persist Security Info=False;")

{

 Dim Conn As OleDbConnection

        Dim Ds As DataSet

        Dim Da As OleDbDataAdapter

        Dim SQL As String = "Select * From ijeoma2"

        Try

            Conn = New OleDbConnection(ConnStr)

            Ds = New DataSet

            Da = New OleDbDataAdapter(SQL, Conn)

            Da.Fill(Ds, "ijeoma2")
```

```
            DataGridView1.DataSource = Ds.Tables("ijeoma2").DefaultView
            DataGridView1.Visible = True
            Visible = True
        Catch
            MessageBox.Show("please ensure you are properly connected....!",
"Database error", MessageBoxButtons.OK, MessageBoxIcon.Exclamation)
            Me.Close()
        End Try
    End Sub
]
    Private Sub Button2_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button2.Click
        Dim ConStr As String = ("Provider=Microsoft.ACE.OLEDB.12.0;Data
Source=c:\Users\user\Documents\ijeoma2.accdb;Persist Security Info=False;")
        con = New OleDbConnection(constr)
        con.Open()
        query = "select *from ijeoma2 where examno='" & TextBox1.Text & "'"
        rdr = reader(query)
        If rdr.HasRows Then
```

```
        da = New OleDbDataAdapter(query, con)
        Dim ds As New DataSet
        da.Fill(ds, "ijeoma2")
        con.Close()
        bind.DataSource = ds
        bind.DataMember = ds.Tables(0).ToString
        Label9.Text = ds.Tables(0).Rows(i).Item(3)
        Label8.Text = ds.Tables(0).Rows(i).Item(1)
        Label5.Text = ds.Tables(0).Rows(i).Item(17)
        Label4.Text = ds.Tables(0).Rows(i).Item(16)
        MsgBox("fingerprint template verified!!authorised users!!")
      Else
        MsgBox("fingerprint template not found")
      End If
    End Sub
End Class
          }
  query = "select *from ijeoma2 where examno='" & TextBox1.Text & "'and
fingerprint='" & Label4.Text & "'"
```

```
rdr = reader(query)
If rdr.HasRows Then
    da = New OleDbDataAdapter(query, con)
    Dim ds As New DataSet
    da.Fill(ds, "ijeoma2")
    con.Close()
    bind.DataSource = ds
    bind.DataMember = ds.Tables(0).ToString
    Label3.Text = ds.Tables(0).Rows(i).Item(1)
    Label8.Text = ds.Tables(0).Rows(i).Item(2)
    Label14.Text = ds.Tables(0).Rows(i).Item(3)
    Label15.Text = ds.Tables(0).Rows(i).Item(4)
    Label16.Text = ds.Tables(0).Rows(i).Item(5)
    Label17.Text = ds.Tables(0).Rows(i).Item(6)
    Label18.Text = ds.Tables(0).Rows(i).Item(7)
    Label19.Text = ds.Tables(0).Rows(i).Item(8)
    Label20.Text = ds.Tables(0).Rows(i).Item(9)
    Label21.Text = ds.Tables(0).Rows(i).Item(10)
    Label22.Text = ds.Tables(0).Rows(i).Item(11)
```

```
                FLabel23.Text = ds.Tables(0).Rows(i).Item(12)

                Label24.Text = ds.Tables(0).Rows(i).Item(13)

                Label25.Text = ds.Tables(0).Rows(i).Item(14)

                FoLabel26.Text = ds.Tables(0).Rows(i).Item(15)

                Label28.Text = ds.Tables(0).Rows(i).Item(16)

                Label31.Text = ds.Tables(0).Rows(i).Item(17)

                Label32.Text = ds.Tables(0).Rows(i).Item(18)

                MsgBox("fingerprint template verified!!authorised users!!")
}
            Else

                MsgBox("fingerprint template not found")

            End If

        Catch ex As Exception

        End Try

    End If
```