DESIGN AND IMPLEMENTATION OF A BIOMETRIC INFORMATION SYSTEM

By

DR. AGBASONU VALERIAN CHINEDUM

DEPARTMENT OF COMPUTER SCIENCE, IMO STATE UNIVERSITY, OWERRI.

PMB 2000, OWERRI, IMO STATE NIGERIA.
PHONE +234803872776
EMAIL.valpraise@gmail.com

ABSTRACT

The objective of this project is to ascertain that by using biometrics it is possible to confirm or establish an individual's identity based on "what she is, rather than by what she posses" (e.g. an ID card) or "what she remembers" (eg a password). And I was motivated because of the wide variety of systems requires a reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their service. The purpose of such schemes is to ensure that the rendered services as accessed only by a legitimate user, and not any one else. Examples of such application include secure access to buildings, computer systems, laptop, cellular phones and ATMs. The methodology that has confirmed this project is by the questionnaire ran interviews, observation, researches and experimentation. In the absence of robust personal recognition scheme, these systems are vulnerable to the wile of an imposter. Biometric recognitions refers to the automatic recognition of individuals based on their physiological and or behavioral characteristics. With this, the results of using biometric system as a security access for any access to any systems or information that is classified, this will be to stop an unauthorized persons having access to the information. In this work, VB Net is a programing language used to develop this project.

1.0 Introduction

The great-break through in technology commonly called "AUTOMATION" is the offspring of the "MANUAL SYSTEM".

Human learned how to input correctly into a machine to recognize, store, process, and give out information as a result. This basic invention opened up a whole new world of technology at the peak of the technology stand the “computer”, it can be programmed to keep in mind a complex set of process, the ability of the computer to handle large volume of high speed data, complex calculation of a higher degree of accuracy has made it a tool in almost all human endeavor such as security, Information security, banking defense to mention but a few.

Establishing the identity of a person is become critical in our vastly interconnected society. Questions like" is she really the right source to the program? Or is this person authorized to use or access the information stored in the computer? The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancement in networking information sharing and security.

This research work is centered on developing a computer based information security; that is biometric support software/program that will allow information access base on the computer system. An individual is prompted
to present their voice, face, and iris or fingerprint sample to the scanner, if it matches to the one on file, the system will automatically open the database for assessment of information.

1.1 Statement of Problem

The utilization of humans mainly "MAN" has the main objective of any establishment because of the large amount of money spent yearly on lost of data and information retrieval. Traditionally, Information security is the act of preventing imposters to have access to the database or information that is secured or classified. This is normally done by pin or password. The manual process entail the availability of password provision to the people that will have access to the base other problem posed by this are;

- Breach of security could lead to lost of organizational stand
- Protecting confidential information is a business/organizational requirement to help protect the free flow of information.
- Access to company/organizational database.
- Lost of important files.
- Protecting the confidentiality, integrity and availability of information.

The problem stated above necessitated the need to change biometric authentication system that will be able to provide more information accuracy and data integrity.

1.2 Objective of the Study

The major aim and objective of this study, is to sanitize/analyze the frequently used information security devices (Pin, Password, etc). Finding out all its pit falls and thereafter develops a computer program that will accept fingerprint biometric security device, and also provide better solution to these discovered problems. Based on the problem of pin/pass wording, other aim and objective of this research are;

- To develop a program that will work with a biometric device and increase accuracy in information access.
- To ensure an advanced technology in security, risk management, reduced cost etc.
- Software that will increase the level of data integrity.
- To enable dissemination of information among system constitutes.
- To increase accuracy in information security.

1.3 Significant of the Study

With the rapid development of the computer technology in virtually all field of operation and the relation of biometric time and information security. It has become important to look into development of a computerized method to meet up with the present day organizational needs. Also, the research will analyze the existing pin/password method of information access in Evan Enwerem University formally known as Imo State University in Owerri, where staffs access information with the use of password and to develop a biometric information security system.

1.4 Scope of the Study

The research work converse the concept of biometric system and information security with much emphasis on the implementation to help evade the problem of most ministers, educational institution, parastatal and private sectors in Nigeria, it also emphasizes on the design of a biometric information security system machines, challenges and benefits to the users. Time, efficiency, value added, security and state of the art technology will be employed and improved database.
1.5 Background of the Case Study

The case study used for this study is Evan EnweremUniversity, located at Okigwe Road Owerri. The university is one of the well-known universities in Nigeria. Imo state University which it was formally known but changed to Evan EnweremUniversity in 2009 was established in 1981 through Law No.4 passed by the Imo State House of Assembly, Owerri. This was amended by Edit 27 of 1985, another in 1988 and finally for the relocation by the Law No. 2 of 1992 Academic activities commenced at the site located at the former Madonna High school, Ihitte with Professor M.J.CEcheruo as its first Vice Chancellor.

Literature Review

Introduction

About the of the 1960s, computers were mainly used as an efficient medium of calculation. With development and sophistication, it found its way in much application in different area of human activities such as sciences, timekeeping, medicine, identification, defense access control etc, the application of computer has gone far more than what the people and early investor of computer did image. Computers are indeed some of the most interesting and complex items of technology in the every day use, but they are only around in such number they are are useful tools computerization and of industries and work plane. It has increased efficiently and effectiveness in the management. The availability of computer and necessary software in operational into every realm of decision making. The first application of computer was tagged data, manufacturing of the collected data, documentation and storage of data. Later, other applications were introduced.

The concept of Management Information System (MIS) and decision Support System (DSS) which attracted the attention of management information specialist in the past two decades or more. The emerges of two new computers and other electronic device in interpersonal communication called Office Automation (OA) and application of computer in aspect of reasoning called Artificial Intelligent(AI) with Expert System (ES) as its subject. The purpose of this section is to examine the views of various experts on computer and computing as it relate to Biometrics Authentication System (BAS). Biometric Authentication System, according to Oxford Advance Learners dictionary (7th Edition) Biometric means using measurement of human factors such as finger or eyes in order to identify people. Osuagwu, O etal (2007) stated that Biometric Authentication system refers to a brand new technology that reliably indicate whether people are actually who they are, using trait unique to them. These traits include fingerprint pattern, the arrangement of tissues in the eye iris and the timbre of a person voice. Business, school and apartment building are using vascular recognition for physical access control; large organizations are also begging to deploy the technology infrastructure. Vein pattern recognition has being adapted to screen passengers at southKoreas international airport, and to control access to the tarmac of several Canadian international airports. Vascular recognition already has won wide acceptance. In biometric time and access control machine an individual is prompted to hold a hand near an infrared light source. The light source is paired with a charge coupled device (CCD) similar to the body tissue; it is related by the homoglobin in the blood. The image create a template that can compare the encrypted image template associated with authentication system with the authorized user and decide whether they match. New technology and changing requirement means that over time the information management in large establishment can become obsolete and out dated or simply loose touch with management. The wide spread use of computer in an establishment has greatly increase the ability to analyze, manipulate
and control large volume of data in order to produce more timely and accurate information for decision making purpose. In view of the application of biometric authentication system in institutions, it is in-dispensable, as it would enhance productivity, efficiency and reliability in institution administrative system in Nigeria.

2.1 Factors Used to Authenticate an Individual

Factors that can be used to authenticate an individual in Biometric Authentication System (BAS) include:

**Something Somebody (person) Knows:**

Commonly a password or pin. If the correct password or pin number is typed access will be granted.

**Something a person has:** Most commonly a physical device referred to as a token. Token include self contained devices that must be physically connected to a computer or devices that have small screen where OTP is displayed which the user must enter into an interface to be authenticated by back end server.

**Something the person is:** Commonly physical characteristics such fingerprint, voice pattern hand geometry or pattern of veins in the user eyes. This type of authentication is related to biometric.

2.2 Variants of biometric authentication

There are many variants of biometric authentication system. But in these studies we will limit our research to the four major variants which includes fingerprint, eyes, iris, facial recognition and speech recognition.

2.3 Fingerprint Recognition

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprint are one of many forms of biometric used to identify an individual and verify their identity. This article touches on two major classes of algorithms (minutia and pattern) and four major sensor design (optical, ultrasonic passive capacitance and active capacitance). The analysis of fingerprint for matching purpose generally requires the comparison of several features of the print pattern. These include patterns which are aggregate characteristics of ridges and minutia points which are unique features found within the patterns. It is also necessary to know the structure and properties of the human skin in order to successfully employ some of the imaging technologies.

2.3.1 Patterns

The three basic patterns of fingerprint ridges are the arch, loop whorl. An arch is a pattern where the ridges enter from the one side of finger. The loop is a pattern where the ridge enter from one side of the finger, form curve and trend to exit from the same side they came in from. In the whorl pattern, ridges form circularly around a circle point on the finger scientists have found that family members often share the same general fingerprint pattern, leading to the belief that these patterns are inherited.

2.3.1 Minutia Features

The major minutia features of fingerprint ridges are: ridges ending, bifurcation and short ridges (or dot). The ridge ending is the point which a single ridge splits in two ridges. Short ridge (or dot) is ridge which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

2.4 Fingerprint Sensors

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted feature) which is stored and used for matching. This is an overview of some of
the more commonly used fingerprint sensor technologies.

2.4.1 Optical

Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the touch surface, beneath this layer is a light emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) which captures a visual image of the fingerprint. A scratched or dirty touch surface can cause the fingerprint. A disadvantage of this type of sensor is the fact that the imaging is affected by the quality of the skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it can also be easily fooled by an image of a fingerprint, if not coupled with a "live finger" detector. However, unlike capacitive sensor, this sensor technology is not susceptible to electrostatic discharge damage.

2.4.2 Ultrasonic

Ultrasonic sensor make use of the principles of medical ultrasonography in order to create visual images of the fingerprint; unlike optical imaging ultrasonic sensors use very high frequency sound waves to penetrate the epidermal layer of the skin. The sound waves are generated using piezoelectric transducers and reflected energy is also measured using piezoelectric materials since the dermal skin layer exhibit, the same characteristics pattern of the fingerprint, the reflected wave measurement can be used to form an image of the skin on the palmer surface of the hand feet forms ridges so called papillary ridges. In patterns that are unique to each individual which do not change overtime, even identical twins (DNA) do not have identical fingerprint.

Fingerprint are typically formed by the fingers and palms, with additional material from sebaceous glands primarily from the fore hand Paul (2007). The latter contamination result from the common human behavior of touching the face and hair. The resulting latent fingerprint consists usually of a substantial proportion of water with a fatty sebaceous components that contains acid.

2.5 Methods of Fingerprint Detection

Since the late nineteenth century, fingerprint identification methods have been used by police agencies around the the world to identify both suspected criminal as well as the victims of crime., The basis of the traditional fingerprint simple, the

2.5.1 Classifying Fingerprint

Before computerization replaced manual filling system in large fingerprint operation, manual fingerprint classification system were used to categorize fingerprint based on getting ridge formation (such as the presence or absent of circular patterns in various finger) thus permitting, filing and retrievals of paper record in large collection on friction ridge pattern independent of names, birth date and other biographical data that person may represent. Reid Donald(2003) popular ten print classification system and the Henry classification system of these system, the Roschers system was developed in Germany and implemented throughout south America and the Henry system was developed India and implemented in most English speaking countries.

2.5.2 Biometric Sensor

Biometric sensors are semi conductor with embedded algorithm that are used in security or environment that require user authentication. They produce electronic signal fingerprint or other physical characteristics in biometric access control system. Biometric sensor consists of analog to digital converter (ADC) that digitalizes information from the sensor array. In fingerprint access control system, the user presses an index finger to a scanning device that includes a
biometric sensor. The varying capture capture values across the sensor array are an image of the fingerprint. Other component of the biometric access control system then compare the image to a stored template.

2.6 Access Control

Biometric system have long been used to complement or replace badges and keys in controlling access to entire facilities or specific areas within a united state employ biometric hand geometric system. As noted in the technology assessment recent reductions in the price of biometric hardware have spurred logical access control application. Fingerprint, iris and speaker recognition are replacing password to authenticate individuals accessing computer and networks. The office of legislative counsel of the US house of representative for example, is using an iris recognition system to protect confidential files and working documents. Other federal agencies including the ~ of defense, department of energy, and department of justice as well as the intelligence nt. are adopting similar technologies. The department of of Homeland security, Transportation Security Administration (TSA) is working to establish system wide common credentials to used across all transportation modes for all personal requiring unescorted physical and or logical access to secure areas of the national transportation system. Such as air port sea ports and rail road terminal called the transportation workers B:Cr credential (TWIC). The program was developed in response to recent laws and will including the use of smart cards and biometric to provide a positive match of a credential to a person for 10-15 million transportation workers across the United State.

2.7 Recognition Errors

There are two basic types of recognition errors, the False Accept Rate (FAR) and the False Reject Rate(FRR). A False Accept Rate is when a non matching pair of biometric data accepted as a match by the system. The two errors are complementary when you try to lower one of the errors by varying the threshold, the other error rate automatically increase. There is therefore a balance to be found with a decision threshold that can be specified to either reduce the risk of FRR. In a biometric authentication system, the relative false accept and false reject rate can be set by choosing a particular operating point (i.e detection threshold) very low (close to zero) error rate both errors (FAR and FRR) at the same time are not possible. By setting a high threshold the FAR errors can be close to zero and similarly by setting a significant low threshold, the FRR rate can be close to zero. A meaning operating point for the threshold is decided base on the application requirements, and the FAR versus FRR error rate at the operating point may be quite different. To provide high security, biometric system operate at a low FAR instead of the commonly commended equal error rate (ERR) operating point where FAR = FRR.

2.8 Compromised Biometric Data

Paradoxically, the greatest strength of biometric is at the same time its greatest liability, it is the fact that an individual biometric data does not change overtime. The r your iris, retina or palm vein remain the same your life, limited number of biometric features (one face, two hands, ten fingers, two eyes). For authentication system base on physical token such as keys and badges, a compromised token can be easily cancelled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as But the biometric features to be used for authentication.

2.9 Vulnerable Point of a Biometric System

The first stage involves scanning the user to acquire his/her unique biometric data. This process is called enrolment. During the enrollment biometric information from an individual is 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 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 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 Date to reduce the file size and to protect the identity of the enrollee. If enrollment is being performed, late is simply stored some where (on a card or within a database or both). If a matching phase is being e. 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 specific use or purpose (e.g. entrance in a restricted area).

This is similar to a password, you first have to create a password for a new user and then when the user tries to access the system, he/she will be prompted to enter his/her password. If the password entered via the keyword matches the password previously stored, access will be granted.

2.10 Attacks

There are seven main areas where attack may occur in a biometric system,

- Presenting a fake finger or a face mask. It is also possible try and resubmitting previously stored digitize biometric signals as a copy of a fingerprint or voice recording.
- Presenting feature sets presentation by the intruder over riding the feature extraction process.
- Tempering with the biometric featured representation, the features extracted from the input signal are replaced with a fraudulent feature set.
- Attacking the channel between the stored templates and the matcher the stored templates are sent to the n c e- through a communication channel. The data travelling through this channel could be intercepted and modified. There is a real danger if the biometric feature set is transmitted over the internet.
- Corrupting the matcher, the matcher is attacked and so that it produces pre-selected match with stored templates, either locally or remotely.
- Overriding the match result.

3.0 RESEARCH METHODOLOGY, SYSTEM INVESTIGATION AND ANALYSIS

INTRODUCTION

3.1 Research Methodology

This is a structured approach or viewing at a dependable solution to problem through the planned and systematic collection, analysis and interpretation of data. Research methodology is a study which is obtained know how the old system worked so that relevant fact will be obtained in order to design the proposed system. It also give a detailed description of what the researcher planned and procedure adopted toward procuring new relevant fact (data). It is the description of subject's instrument, design, procedure, assumption and limitation. The description of subject includes a determination and description of the population
from which the sample was selected the method used in selecting them or samples.

3.2. Data Collection Method

There are two major ways in which data can be collected; they are primary and secondary method of data collection. The primary method is a method through which the firsthand information or fact could be obtained it includes interviews, questionnaire, observation, site visitation and experimentation and secondary methods like textbook, newspaper, magazines, journals, periodicals, textbook, conference proceedings, seminar papers.

3.3 System Investigation/Analysis

System Investigation: This involves the research into the objectives problem and opportunities of the present and proposed system (EtifitE.E 2001) introduction of system development page 21. It refers to making of research into the objective of a system making research/finding into the problem and difficulties encountered in a study. There are two major aim of studying the system.

- To determine if a problem actually exist in a system.
- If the problem exists, whether there is a feasibility (practical) solution.

3.4 Analysis of Existing System

The research was based on analyzing the traditional systempass wording system which involves each user singing or log in into the system. According to George Beckman (1997), he defines system analysis as the gathering of document, interviewing user of current seem (if one exist) observing the system in action and generally gathering and analyzing data to help understand the current system and identifying new requirements. EtifitE.E (2001) said that system analysis is the process of breaking a problem into smaller unit for a close study of the individual port individual port; it is aimed at the examining the organizational system to see if the system needed more modification or improvement in performing its function.

System analysis, is the study of a system problem domain to recommend improvement and specify the system requirement for the solution, It is also the dissection of a into its components piece to study how components these pieces interact and worked. However, the system was analyzed based on its in efficiency, effectiveness and security. Issues on the application of information security; this phase is a detailed approval of the existing system, which includes finding out how the system works and what it does. It also include finding out in more detailed approval of the existing system problem are and what users required of any new or changed system. Finally, it involves the definition of business requirement and priorities for the proposed system.

3.5 Objective of the New System

The aim and objective of the new system include the following:

- Are there any major barriers of information access?
- If any how can such problem be solved?
- What is the access control like?
- What is the security control like?

3.6 Analysis of Existing System

This primary objective of analyzing the existing system is to ascertain the strength and seeing weakness of assessments, retrieving, creating of information of the establishment involved.

Withthe aim or, recommending, installing and linking to a system that is much as possible improve the establishment operational effectiveness and efficiency. In other to achieve this solution the following questions could eat help.

- Are there any major barriers of information access?
- If any how can such problem be solved?
- What is the access control like?
- What is the security control like?

3.5 Objective of the New System

The aim and objective of the new system include the following:

To design a system that will be flexible ie a system that can adapt to change in the information need.
To design a system that will satisfy user requirement.
To design a system that process information faster and easier.
To design a system with great access control topology.
To design a system with better security than the earlier method.
To design a system with much electronic control.
To design a system with a security base with biometric security.
To develop a computer security development system with biometric system.
To design a system with great authentication with a powerful device (Biometric Fingerprint Reader).

SYSTEM DESIGN AND IMPLEMENTATION

4.0 INTRODUCTION

The analysis of the null description of the existing system and the objective of the proposed system should lead to a full specification of the user requirement. This requirement specification can be examined and approved before system design is embarked upon. The purpose of the design stage is to work from the requirement specification to produce a system specification that will be a detailed set of document which provide details of all features of the system. Jane Hale (page 151) gave an insight into what is expected of system analysts when she said "I'm not expecting to come with the best possible design but what I want is a workable design" that fits the task(s), fits the people and design should not be out data next year. Here the statement calls for an efficient design hinged on meeting user's requirement and goal of the organizations.

4.1 Input /Output Design

The input to the new system consists of the various authentication type, i.e. fingerprint, iris, voice prompt, facial signature etc. The samples are labeled according to the type of input and also verify to determine its validity and integrity.

The outputs are the processed information which includes the recorded data. The output will be design in such a way that will accept data process it and store the information of every staff for accurate and effective access control.

4.2 System Specification

This is a process of specifying the user requirement, it also include feature like acceptability, efficiency, accuracy, completeness, capabilities, authorization, authentication, security risk, universality, uniqueness, computer security. There is greater need that accurate and complete specify characteristics of the new system.

4.3 System Flowchart

A system flowchart is an important tool for system analysis. It is a graphical representation of the steps necessary to solve a problem, complete a process, accomplish a task, it is use to illustrate the component of of system. Most cases we use a flowchart to illustrate the in which a variety of decisions are to be made and activities performed.

Programming Language Used

The programing languages used in the development of project work are Visual basic. Net. It has better assessment capability for net connectivity.
It is possible if human characteristics can be used for biometric in the terms of the following parameters:

- Universality: Each person should have the characteristics.
- Uniqueness: Is how well the biometrics separates performance.
- Collectability: Ease of acquisition for measurement.
- Performance: Accuracy, speed, robustness of technology used.
- Acceptability: Degree of Approval of a technology.
- Circumvention: Ease of use of a substitute.

A biometric system can operate in the following modes:

- Verification: A one to one comparison of a captured biometrics with a stored template to verify that the individual is who he claims to be can be done in conjunction with a smart card, username or ID.
- Identification: A one to many comparison of the captured biometric against a biometric database in the attempt to identify an individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.

4.4 Program Design

The program is designed to take care of the respective task that constitutes the biometric information security system and its implementation, the program design is based on the input and output specification facilitate easy coding, testing, debugging and it is in module, the database used is Microsoft Access, while the programming language used is Vb.Net, and its execution and explanation will be on pieces with Windows operating platform.

4.5 Program Design

The program is designed to take care of the respective task that constitutes the biometric information security system and its implementation, the program design is on the input and output specification facilitate easy coding, testing, debugging and it is in module, the database used is Microsoft access, while the programming Net, and its execution and implantation will be on pieces with Windows operating platform.
5.0 Introduction
In information development security, Biometric Authentication System (BAS) refers to a brand new technology that will reliably indicate WHETHER people are actually who they are because reliable personal recognition is critical to many business processes. Biometric refers to automatic recognition of an individual based on her behavioural and or physiological characteristics. The conventional knowledge based and token based methods. Thus biometric Authentication System (BAS), information Security that implemented into the University will provide staff with most security and helps in Information Security to confidential data's.

5.1 Conclusion
Biometric comprises methods for uniquely recognized humans based upon one or more intrinsic physical or behavioural traits. In Computer Science, in particular Biometric is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric Characteristics can be divided in two main classes:

- Physiological are related to the shape of the body e.g. include, but are not limited to fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition, which has largely replaced retina and odour/scent.
- Behavioral are related to the behavior of a person. Example includes, but is not limited to typing rhythm, grail and voice.

Sameresearchers have coined the term behavior metrics for this class of biometrics. Strictly speaking, voice is also a physiological trait because every person has a different vocal tract, but voice recognition is mainly based on the study of the way a person speaks, Commonly classified as behavioural.

Biometric refers to automatic identification of a person based on his/her physiological or behavioral characteristic. It provides a better solution for the information society than traditional identification methods such as passwords and pins. As biometric sensor becomes less expensive and miniaturized and as the public realizes that biometric is actually an effective strategy for protection of privacy and from fraud, this technology is likely to be in almost every information needing authentication of personal identity.

5.2 Recommendations
Having gone through examination of the existing system (password or Pins) in Evan Enwerem University Owerri and in view of the numerous
advantages association with the use of computer and the biometric Authentication system (BAS) fingerprint in particular. I believe that the advent of Biometric information security with fingerprint em will be of greater advantage when implemented in Nigeria.

Therefore I recommend this project work on information security using biometric System to be implemented in Nigeria by:

- Private sectors
- Government (Federal, State and Local government Areas).
- Pension Scheme


**Websites**

- www.biometric.com/iris
- www.biometricbits.com/iris.challenge.htm
- www.biometricgroup.com/report
- www.scafe.org/library/1.60201.htm
APPENDIX