Multimodal Authentication Techniques For Staff Identification And Tracking

Overcomer Anusiuba Ifeanyi, Anigbogu S.O., Onyesolu Moses, Okonkwo
E-mail: oifeanyi@yahoo.com Phone No: +234-8035509616
Computer Science Dept. Nnamdi Azikiwe University Awka

Abstract

It is obvious that most establishments are faced with security challenges. Consequently securing and protecting our identity and valuable data have become areas of great concern which cannot be ignored. Continual quest for a more authentic solution to track, verify and checkmate amongst others, staff movement within an organization, their dedication to duty and a logical system of wading off intruders. Multimodal Authentication Techniques is an option for an improvement. It creates a greater level of assurance of an accurate match in authentication, verification, tracking and identification systems. It helps to overcome limitations of single biometric solutions to reduce the ability for the system to be tricked fraudulently. It is best, most efficient, effective and most reliable when Biometric Technique and Magnetic Coded Swiping Card or Barcode Reader Technology is combined. A Hybrid of Structured System Analysis and Design Methodology (SSADM) and Object Oriented Analysis and Design Methodology (OOADM) was used. The software was developed using Microsoft Visual Basic Programming Language, and Microsoft Access as the database. A parallel changeover was also recommended after deployment to avoid the disruption of the existing processes.

1.0 Introduction

The increasing use of technology and global events has significant impact on the world today. A more interactive and virtual society has emerged through the use of Internet and, as a result, has exposed individuals and businesses to a host of security issues. Because of this, securing and protecting valuable data and our identity have become areas of great concern and cannot be ignored.

Clearly, it has become critical in today's environment to implement ways to increase security levels. Maintaining and managing access while protecting both the user's identity and the computer's data and systems has become increasingly difficult.(**Hopkins,1998)**

Furthermore Authentication that addresses "**something you are**" is a much stronger internal control over other types. Authentication types such as "**something you know**", for instance passwords, have been increasingly difficult to manage. Recently, individuals have become overwhelmed with the number of passwords that must be remembered on a daily basis. We each have multiple accounts and use multiple passwords on an ever-increasing number of computers, applications and websites. (**Jain., 2007**)

As the number of passwords increases, their effectiveness declines. For example, individuals may have to remember at least six passwords before beginning their work. Some companies require a password to enter the premises, to enter the building, to enter their departments within the corporation, to logon to their computer, turn off a screen saver, and also to check their voice or electronic mail. As you can see, this can be challenging for the average user. A typical office scenario consists of workers with multiple notes containing passwords nearby their computer, which defeats the purpose of having a password. Forgotten passwords also can be extremely costly for corporations in that they must hire help desk workers, whose sole purpose is to reissue passwords to forgetful individuals.

Additionally, a major weakness with "something you have" is that these keys and smart cards can be misplaced or stolen, causing security vulnerabilities. Ultimately, the trouble with these methods is that they really only test whether the secret knowledge or special possession is present, not whether its rightful owner is.

Biometric technologies can be used to identify people by pairing physiological or behavioral features of a person with information which describes the subject's identity. It is almost impossible to lose or forget biometrics, since they are an intrinsic part of each person, and this is an advantage which they hold over keys, passwords of codes. These technologies, which include amongst others, face, voice, fingerprint, hand and iris recognition, are the basis of new strong identification systems.

However, biometric technologies are still largely under development despite the fact that they have been used in various applications over the past 40 years. In addition, they form only part of an identification system. There are challenges for such systems, on the one hand emerging from the need to adequately protect them from abuse, and on the other as a result of their wide-scale implementation and the impact that may have on society. There is currently a lack of data and research relating mainly to the non-technological challenges and more specifically to the large-scale introduction of biometric identifiers, including their use in visas, residence permits and passports.

2.0 Literature Review

Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity. The increasing demand of enhanced security systems has led to an unprecedented interest in biometric based person authentication system. Biometric systems based on single source of information are called unimodal systems.

Although some unimodal systems have got considerable improvement in reliability and accuracy, they often suffer from enrollment problems due to non-universal biometrics traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data. Hence, single biometric may not be able to achieve the desired performance requirement in real world applications.

One of the methods to overcome these problems is to make use of Multimodal Authentication Techniques, which combine information from multiple modalities to arrive at a decision. Studies have demonstrated that multimodal systems can achieve better performance compared with unimodal systems. (Hong and Jain, 1998).

Furthermore, Reliable user authentication is essential. The consequences of insecure authentication in a banking or corporate environment can be catastrophic, with loss of confidential information, money, and compromised data integrity. Many applications in everyday life also require user authentication, including physical access control to offices or buildings, e-commerce, healthcare, immigration and border control, etc.

Currently, the prevailing techniques of user authentication are linked to passwords, user IDs, identification cards and PINs (personal identification numbers). These techniques suffer from several limitations: Passwords and PINs can be guessed, stolen or illicitly acquired by convert observation.

In addition, there is no way positively link the usage of the system or service to the actual user. A password can be shared, and there is no way for the system to know who the actual user is. A credit card transaction can only validate the credit card number and the PIN, not if the transaction is conducted by the rightful owner of the credit card.

Finally, the tremendous world-wide interest in intelligent biometric techniques in fingerprint and Barcode Reader is fueled by the myriad of potential applications, including organizations, multinational Companies, banking and security systems, and limited only by the imaginations of scientists and engineers. This growing interest poses new challenges to the fields of expert systems, neural networks, fuzzy systems, and evolutionary computing, which offer the advantages of learning abilities and human-like behaviour. (Jain, 2007).

The Multimodal Authentication Techniques in Fingerprint and Barcode Reader presents a thorough treatment of established and emerging applications and techniques relevant to this field so rich with opportunity.

Objectives of the Study

The following formed the Objectives of this work

1. To provide a more accurate and reliable user authentication method for identification and tracking of staff.
2. To create a platform for an authentication system that cannot be shared or tricked fraudulently. (**NB: credit card**)
3. To improve on the following existing user authentication techniques
   - Something you know, e.g. password or PIN.
   - Something you have, e.g. key.
   - Something you know and have, e.g. card + PIN
   - Something you are, e.g. fingerprint, hand, iris, retina, voice.
4. To combine the Magnetic Barcode and Biometrics technologies to create a more reliable authentication system.

3.0 Methodology

The methodology adopted is a Hybrid Methodology, the **Structured System Analysis and Design Methodology (SSADM)** to help in investigating the existing system and **Object Oriented Analysis and Design Methodology (OOADM)** to help in the development of the new system.

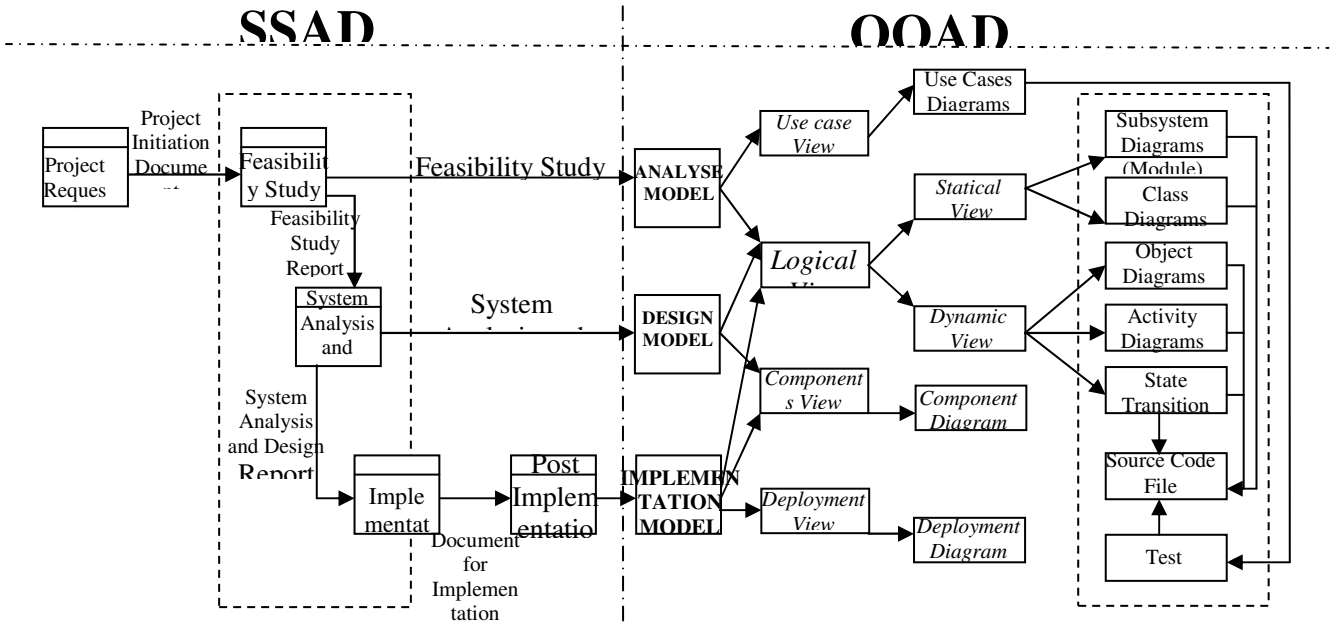


Figure 1: The Hybrid Methodology Of Ssadm And Ooadm

Dataflow Diagram of Existing System

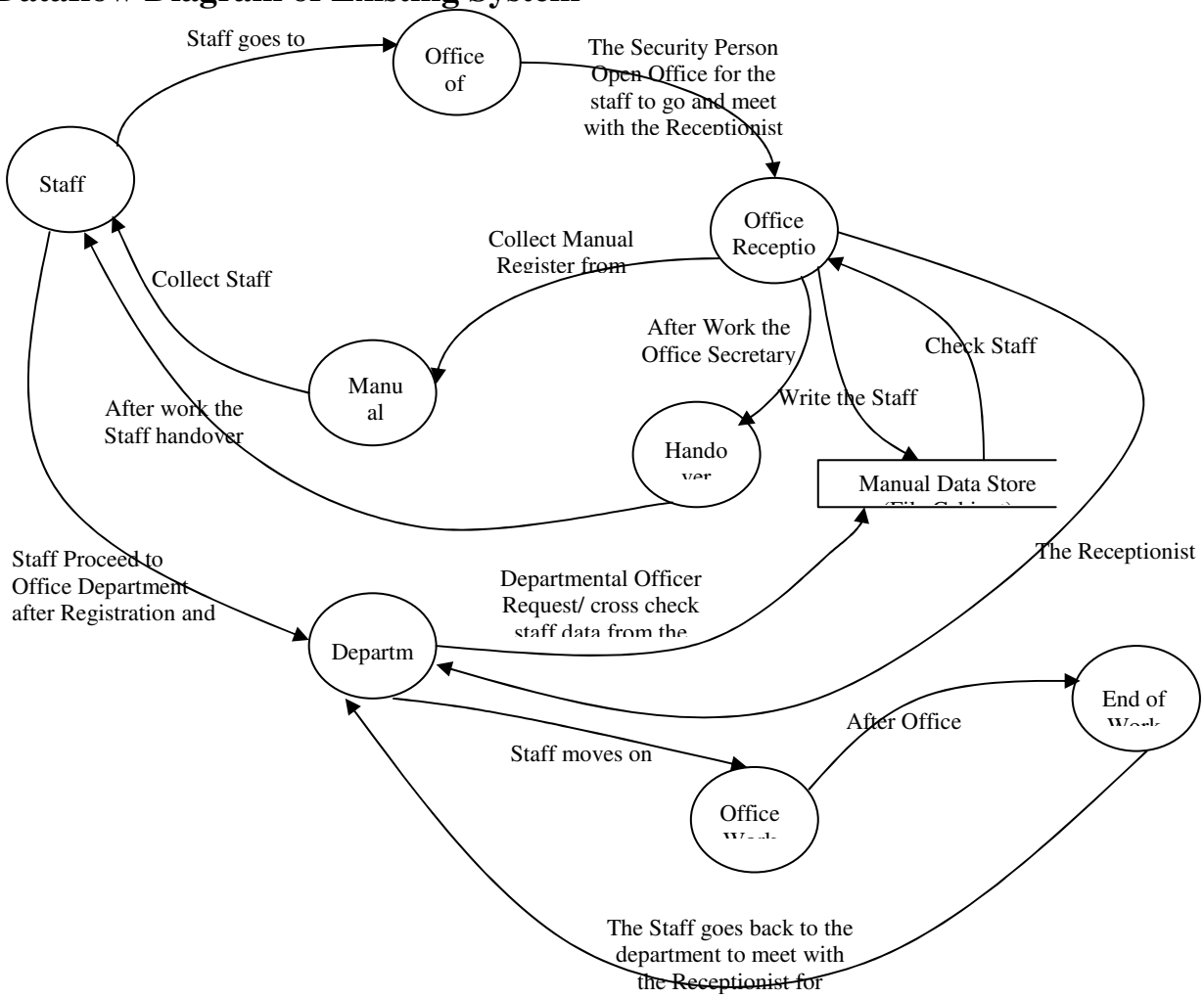


FIGure 2: **The DFD of The Existing System**

The Dataflow Diagram Of The Envisaged System

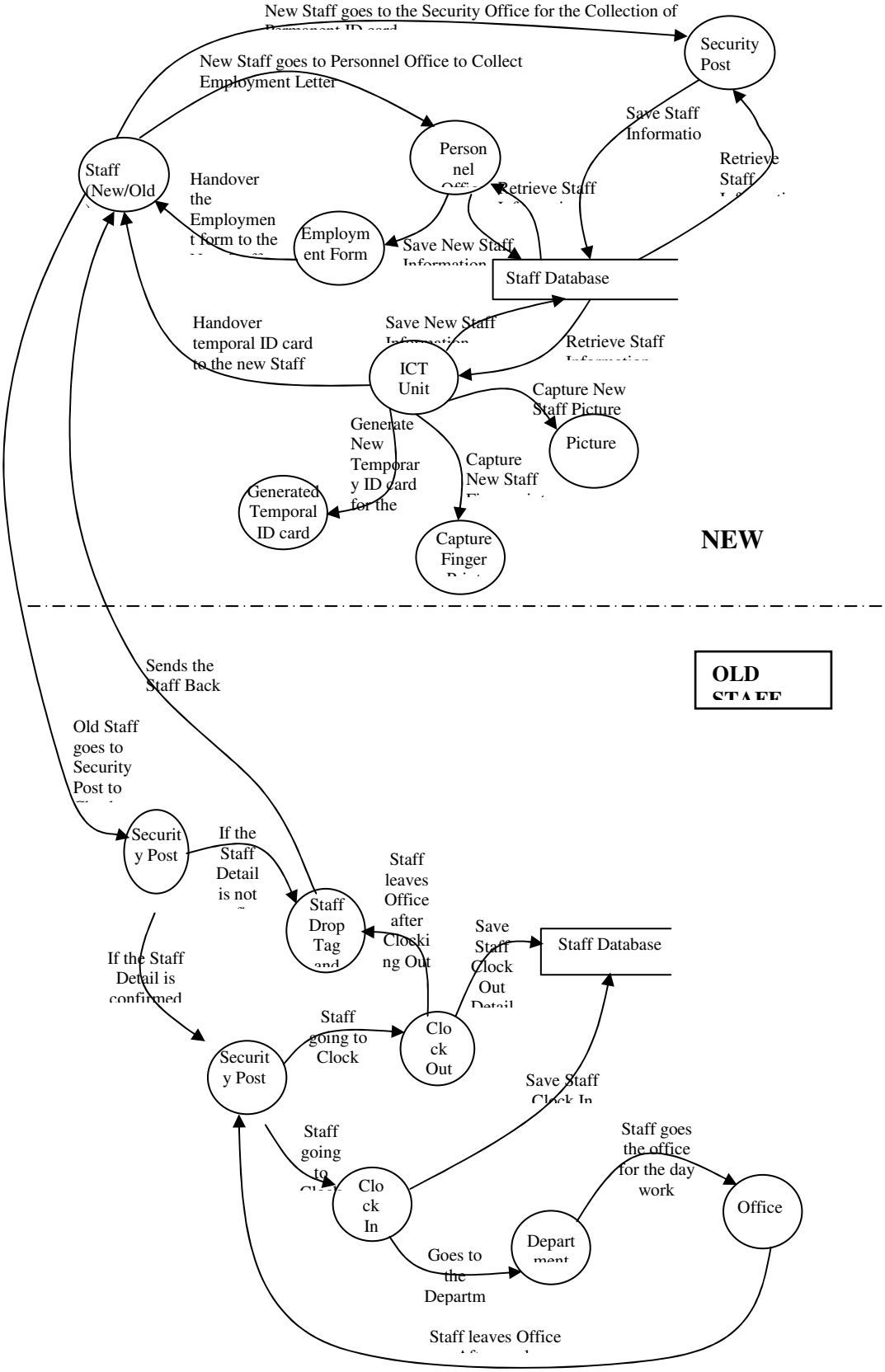


Figure 3: DFD of The Envisaged System

4.0 System Design

The Overview of The Envisaged system

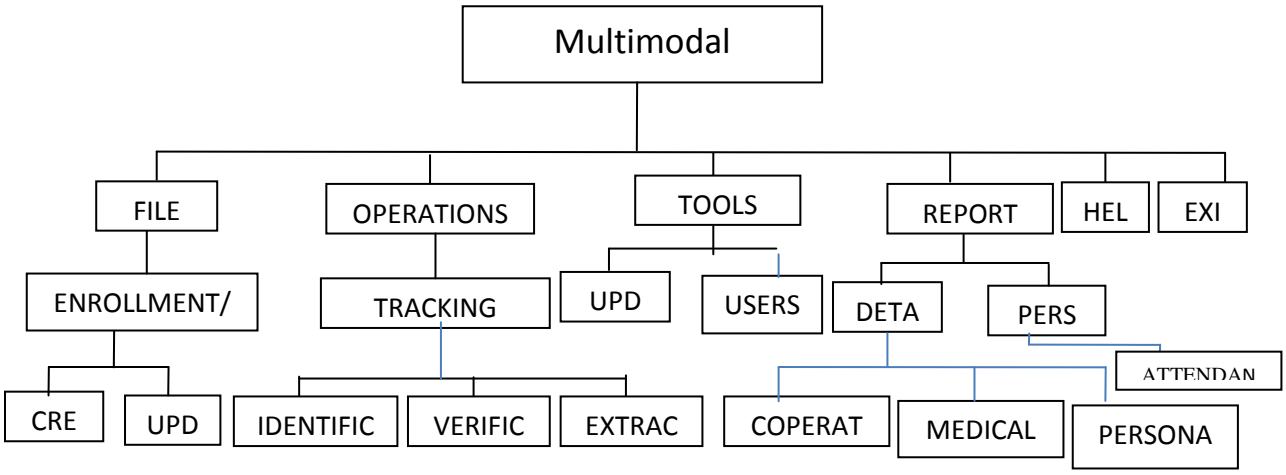


Figure 4: High Level Model of The Proposed System

Design Approaches

The design of the project is carried out based on the following guidelines:

- Database Design and Specifications
- User's Module
- Admin Module
- Input / Output Specifications
- Input Specification and Design
- Output Specification and Design

The Overview of The Enrolment Task

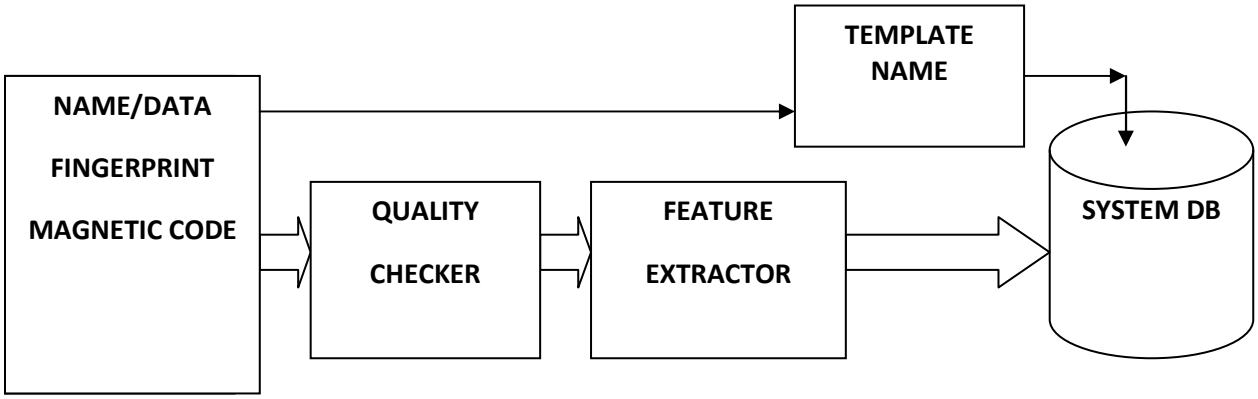


Figure 5: The Overview of The Enrolment Task

The Overview of The Verification Task

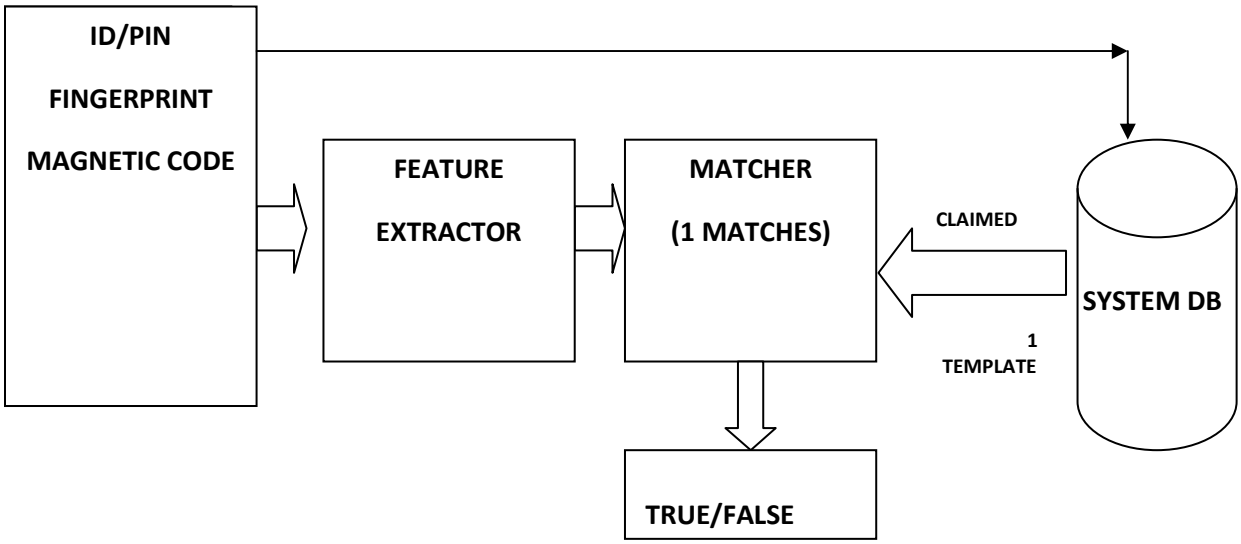


Figure 5: The Overview Of The Verification Task

The Overview of The Identification Task

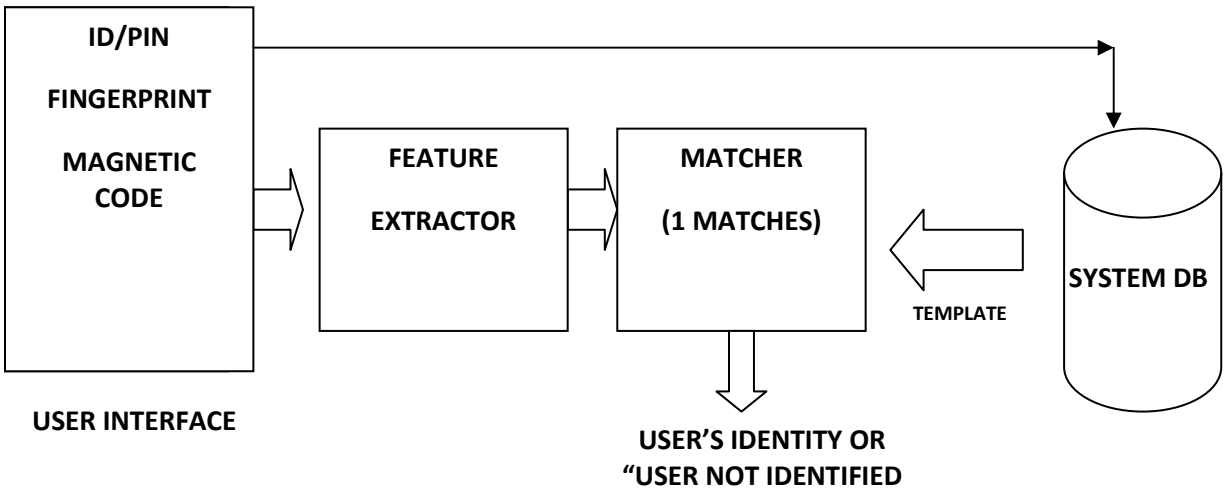


Figure 6: The Overview of The Identification Task

Program Flowchart Diagram Of The Proposed System

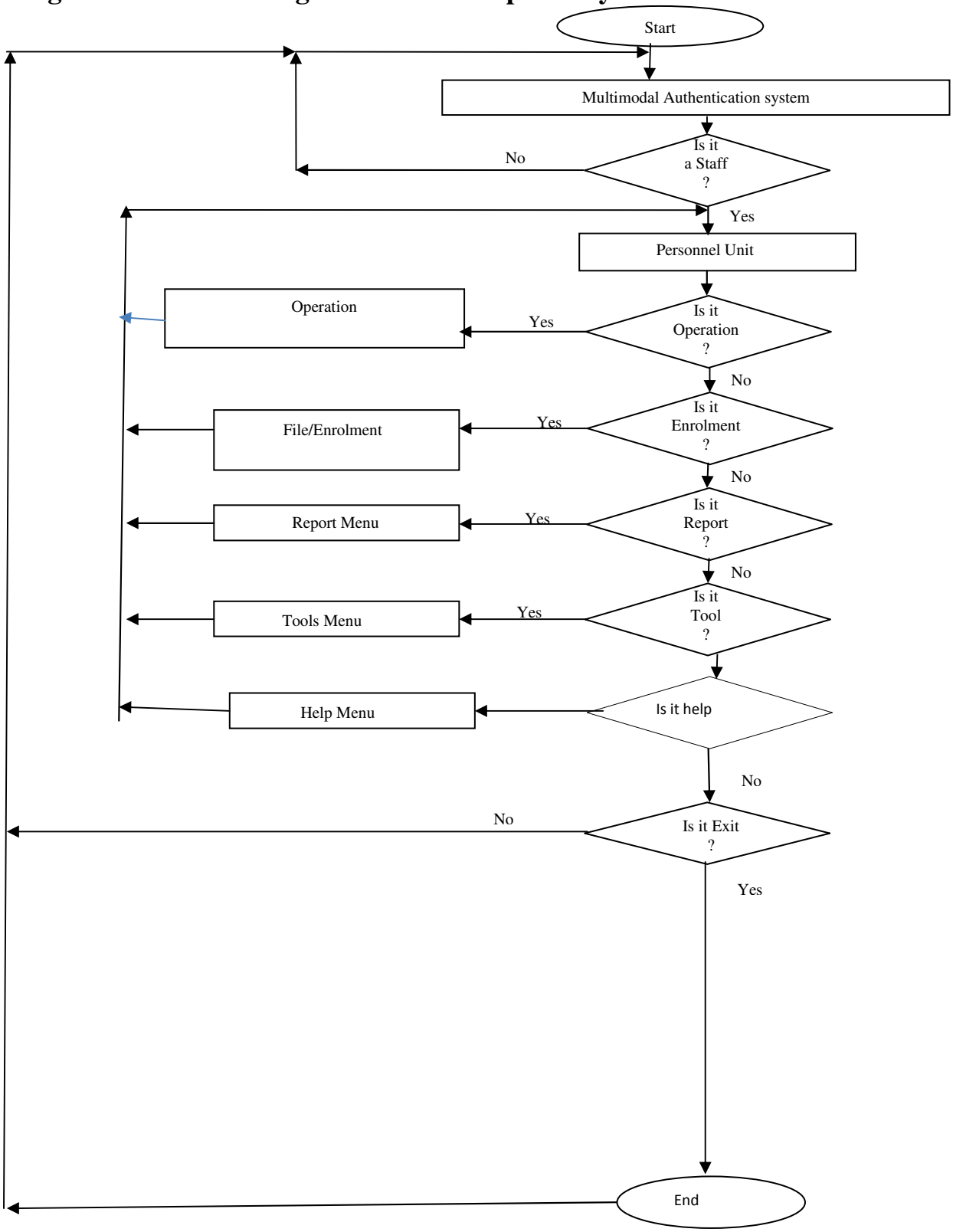


Figure 7: Program Flowchart Diagram of The Proposed System

Program Module Specification

The entire system was broken into subsystems. Each subsystem was designed to interoperate as a single module. The application has six basic steps:

- Authentication of users to filter unauthorized access.
- Initializing the fingerprint and Magnetic card reader.
- Capturing of staff personnel, cooperate, and medical information.
- Enrollment of staff fingerprint using the SECUGEN fingerprint scanner.
- Extracting a template for each fingerprint image.
- Swiping a magnetic card and linking it to the corresponding staff record.

Input/Output Format For The Program

The input/output to the system is designed to be accepted from electronic keyboard, webcam/digital camera, fingerprint reader, any magnetic card reader. Through the keyboard and reader, data is fed, and the result of the processing is stored. The input to the system values with field name.

.

Field Name	Data Type	Field Width
Staff ID	VarChar	50
Barcode	nVarChar	150
Surname	nVarChar	50
Middle Name	VarChar	50
Sex	VarChar	6
Date of Birth	DateTime	8
EmployeeNo	VarChar	20
CompNo	VarChar	20
MinDeptAgency	VarChar	50
Rank	VarChar	20
GradeLevel	VarChar	20
GSM NO	VarChar	20
LocalGovt	VarChar	20
StateofOrigin	VarChar	20
HomeAddress	VarChar	50
Image1	Image	
Image2	Image	

Sgf Plibx.Ocx Active X Control

The SGF PLIBX.OCX provides the user device facility and extraction and verification algorithms. All SDK functions are integrated with SGF PLIBX.OCX.

The SGF PLIBX.OCX is comprised of two controls, which you can use to access almost all functions in the SDK:

- FPLIBX capture (captures image data and extracts minutiae data from it)
- FPLIBX verify (compares and verifies minutiae data with the stored minutiae data)

Creating The Sgf Plibx.Ocx

This active X control can be added by selecting "SGFPLIBX Active X module "from the components pallet". The FPLIBX capture and the FPLIBX verify are added automatically.

Destroying Sgf Plibx.Ocx

The control is automatically deleted from memory when the program exits.

Opening Device

To initialize (open) the fingerprint reader the device type in the Code Name property is set

Image Capturing Operation
Fingerprint images are captured from the reader using the CAPTURE ( ) method

Registration
The GetMinutiaeData ( ) method is called to extract minutiae data from a fingerprint image. The extracted minutiae data is stored in the image1 and image2 fields of the staff info table in the database.

Verification
The VerifyEX ( ) method is called to match new minutiae data to the two sets of registered minutiae data. It has three parameters: - Two registered minutiae data and the minutiae data to be matched.

Writelog
This is triggered by each message generated by class

Fingerprint Capture Overview

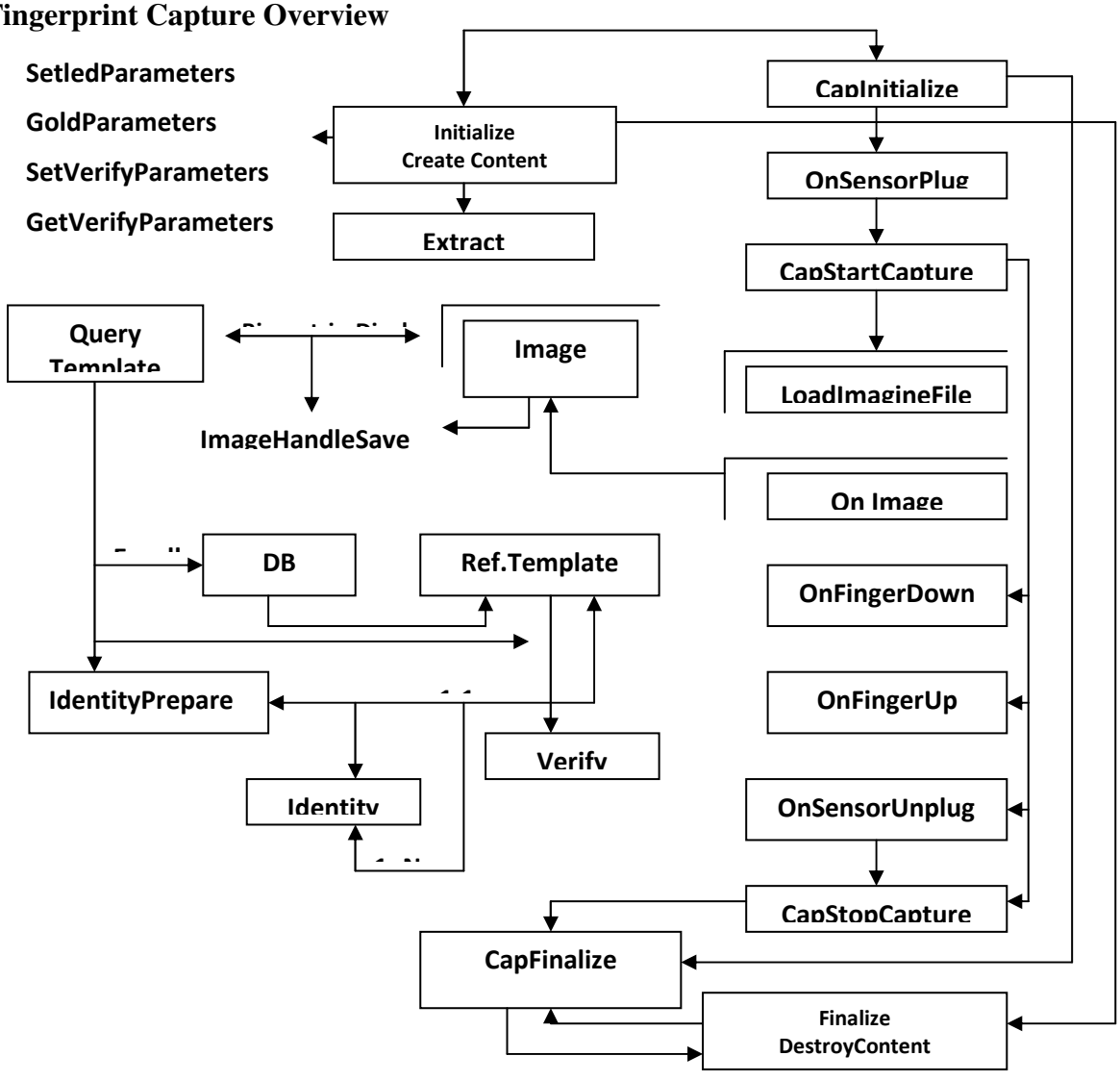


Figure7: Finger Print Capture Overview

The Minutiae Psedocode

```
Function MATCH-SET (Source-minutiae-list, target-minutiae-list)
        Return success or failure
Input:
        Source-minutiae-list, a list of minutiae
        Target-minutiae-list, a list of minutiae
Source-pairs  ←————  GENERAL-PAIRS (source-minutiae-list)
Target-pairs  ←————  GENERATE-PAIRS (target-minutiae-list)
        SORT (source-pairs); sort by distance ascending
        SORT (target-pair);
        NEXT-source-pair:
For             each x Є source-pairs
        NEXT-target-pair:
If tparams  ←————  EXTRACT-TRANSFORMATION-PARAMS(x, y)

DO-ROTATION-ON-SOURCE-DATA (tparas.translation)
        DO-TRANSLATION-ON-SOURCE-DATA (tparas.translation)
IF      EXIST-SUFFICIENT-MATCHES (source-minutiae-list,target-minutiae-list
        Returns (success)
ELSE
        RESTORE-ORIGINAL-SOURCE-DATA ( )
        GOTO next-target-pair
ELSE
        GOTO next-target-pair
ELSE
        GOTO next-source-pair
RETURN failure
```

5.0 System Implementation

The new system must be implemented or installed in the organization, and its operation must be evaluated to ensure that it fulfills its design specification. Documentation involves requirements to run the current systems and other descriptive information in form of manual that explains the use and operation of the system. It is a bi product of the program writing process which aids maintenance of the program during its lifetime. It is a reference manual for the users of the system.

Choice Of Programming Language

The source program was developed with a combination of Visual Basic 6.0 and Structured Query Language (SQL) and Microsoft Access as the database. The choice of Visual Basic was influenced by its flexibility with Windows Operating System and a very good interaction with MS SQL Server. The fingerprint SDK ActiveX component is fully supported by IDE of Microsoft Visual Basic.

Hardware And Software Requirement

The hardware requirements for the implementation of this system are:

A. A complete Computer System with the following configuration.

- Pentium 4, 2GHZ and above processor.
- 40 GB Hard Drive and above space required.
- 512 MB RAM and above.
- 1074x768 Screen resolution monitor.
- Enhanced Keyboard.

B. Fingerprint Reader

- Secugen Hamster III Fingerprint was used for this research.

The system has ability to support other readers

C. Any plug and play Magnetic Card Reader or Swiping tool is supported.

The Software requirements for the implementation of the system are:

- Microsoft.Net Framework version 3.5 and above.
- MS SQL server 2000 and above.
- Secugen SDK.
- Cross Match device driver / the supported reader driver.
- Microsoft Operating System XP/Vista, Windows 2000 server and above.

Installation And Configuration

To install the designed application, open the folder "BIOPERSONNEL" from D: drive, if it is not auto run then copy folder to Drive C:

- Double Click the folder.
- Click on "BIOPERSONNEL AUTHENTICATOR" or right click to open.
- The program will be initialized
- Press F5 to execute the application

NOTE: The following would have been installed on the system, the Fingerprint SDK, MS SQL Server 2000 and above and the Driver of the Reader.

System Test

To test the application, upon execution of the program as described above, you would notice the interface with forms that should be populated with personnel Bio-data, and capture the user biometrics.

To connect the database the default name SA and the Password is "OVERCOMER".

Hence the overall purpose of designing the system is for authentication of user on presentation of a fingerprint and Magnetic Swipe card and to log them in for work. It therefore implies that the result of verification, of 'accept/reject' the user is a major output expected from the system and display on the status bar. This is obtained after all processing activities have been completed, result is written to log file which can be display on screen or point out.

The Changeover

When the new system is proved to be correct, a double cycle in one period makes the pilot runs parallel runs. In this sense the changeover recommended is THE PARALLEL CHANGEOVER because it will allow the organization to still use the old system alongside the new system for a period of time, to avoid risk of direct changeover. The old system can be abandoned in the knowledge that extensive checking of the new system has been carried out.

6.0 Results And Discussions

Summary

Biometric and Magnetic Barcode or Swiping Card system eliminates unreliable methods use to identify humans for specific purpose. In order to have a fast, reliable and secured process of capturing and verifying Niger Delta Development Commission the Multimodal Authentication Techniques is introduced and it is better to have the system customized.

It is obvious, that the manual process of record keeping system in the public sector where existence of multiple files relating to the same employee makes it difficult to determine which records to use to verify personnel for establishment is very vulnerable.

The Multimodal Authentication Techniques no doubt offers a more secured automated method to authenticate identity since one cannot loose, forget or share their biometric recognitions most especially where the biometric is combined with another techniques.

Related Literatures and Overview of concept was reviewed. Biometric vulnerabilities are defined so that they can be mitigated before clever manipulation uses them. The study serves to introduce, define security considerations and highlights best practices to adopt by organizations for the implementation of biometric system. The old method was

analyzed and the design of the new system takes advantage of the idea to capture biometric data using the fingerprint trait and a Magnetic Swiping Card for Authentication.

Review Of Achievements

The developed Multimodal Authentication Techniques is a successful application in actualizing human pattern recognition. It has features of reliability, flexibility and improved scalability. It is complainant with available industry standard that ensure biometric data interchange and interoperability. Its wide range support of fingerprint readers and template consolation, improved recognition rate and eliminating the need of using only a Magnetic Swiping Card and multiple samples of the same finger and outstanding fingerprint matching speed is a major achievement

Contribution To Knowledge

- The developed Multimodal Authentication Techniques will be a successful application in actualizing human pattern recognition. It has features of reliability, flexibility and improved scalability
- Multimodal Authentication Techniques provides more accurate and reliable user authentication method and reduces the ability of the system to be tricked frequently. Therefore Multimodal will be a better alternative.

Areas Of Application

Pattern recognition has found applications in different spheres of business, engineering, science and computing. Some of the application areas are in automated diagnosis, transportation in the airport security and financial in the use of smart cards for business Transactions. However, Multimodal Authentication Techniques as a security measure for personnel access control and identity verification can be integrated to the state payroll, pension funds amongst other systems.

Suggestions For Further Studies

Further research for the use of biometrics system in organization should be done in the area of Multimodal Biometric combining two or three biometrics; the video clips can also be studied for matching identity. Also to improve the actual pattern used for biometric recognition, further research should be conducted regarding algorithm development template protection, and error rate estimation.

Furthermore, system testing and evaluation on large database would help judge the exact scalability of the implementation of a national database.

Recommendation

Multimodal Authentication system should be encouraged by the public and private sectors of the economy. On development of this application, only accurate data should be captured into the system.

The use of this Multimodal Authenticator should be evaluated and adopted by different organs of government.It is important for employees to be informed and educated about the scope of the use of Multimodal Authentication data collected to allay any privacy fear or concern.

A process should be put in place to ensure that enrollment takes place in a manner that does not inconvenient employees or slow down ongoing operations within the organization. There are currently some social, political and ethical concerns that make this model unattractive. As a result the legislative and judicial branches of the Federal Government must provide more clarity on how multimodal Authentication information will be implemented, monitored and legislated.

Conclusion

The research work has theoretically and practically demonstrated how the Multimodal Authentication system can be made much easier than the traditional method of verifying an individual.

As evidenced in the operations of public sector where paper records of personnel are replicated in many establishments and do not prove effective means for positive identification, giving room for manipulations and embezzlement of funds, fake identity or ghost workers. The Biometric solution provides a better alternative.

Conclusively, when this application is fully deployed, it will save time, provide positive identification, the application will serve as a data repository for any Governmental establishment in Nigeria and can be integrated to payroll, pension funds amongst other systems.

REFERENCES

[1] Aladjem M.I. Dimitrov, S. Greenberg and D. Kogan, (2000): *Fingerprint Image Enhancement using Filtering Techniques,* Pattern Recognition, 2000. Proceedings. 15th International Conferences, Vol. 3, pp. 322-325, 2000.

[2] Babita Gupta (2008): *Biometrics: Enhancing Security in Organizations,*E-Government/Technology Series Report 2008, p9, IBM Center for: The Buisness of Government Washington DC 20005.

[3] Bolle R.J. Connell, S. Pankanti, N. Ratha and A. Senior, (2004): *Guide to Biometrics* New York: Springer, 2004.

[4] Bonsor K (2001): *How Facial Recogniton Systems Work,* 2001: Springer- Verlag, New York.

[5] Bruderlin R. (2001): *What is biometrics?* Paper, 1999-2001. Springer-Verlag, New York.

[6] Bush, G.W. (2004): *Homeland Security Presidential Directive/HSPD-12.* Retrieved on Jan.10,2008 from http://csrc.nist.gov/drivers/documents /Presidential-Directive-Hspd-12.html

[7] Carrillo, C.M (2003): *Continuous Biometric Authentication,* a proposed design, Naval Postgraduate School, Monterey, California. P2, p39.

[8.] Chiemeke, C. Stella and Egbokhare, A. Franca (2006): *Principles of Sytem Analysis and Design,* Root Print and Publishers, University of Benin Benin City, pp 117, 119 and 126.

[9] Dalal, N. (2007): *The Global Biometrics Market,* Report excerpt retrieve On Jan.8,2008,from http://www.bccresearch.com/RepTemplate \ . cfmreported=694&RepDet=HLT&cat=ift&target=repdetail.cfm

[10]. Daugman, J. (2006): *Probing the Uniqueness and Randomness of Iriscodes: Results from 200 billion Iris code Comparisons.* Proceedings of IEEE, 94 (11), p. 1927-1935.

[11] Daugman, J. (2000): *How Iris Recognition Works,* Springer-Verlag, New York.

[12] Ejiofor V. (2008): *Lecture Notes* on Software Development And Management, Dept of Computer Science, NAU (unpublished).

[13] Esser, M. (2000): *Biometric Authentication, Essay, October 2000.Info Magazine, New York.*

[14] Faulds, H. (1880): *On the Skin-Furrows of the Hand.* Nature, 22, pp.605.

[15] Galton, F (1888): *Personal Identification and Description.* Nature, 38, p. 201-202.

[16] Herschel, W (1880): *Skin Furrows of the Hand.* Nature, 23, pp.76.

[17] Hong L. and Jain A.K. (1998): *Integrating Faces and Fingerprints,* IEEE Trans. Pattern Anal. Machine Intell., Vol. 20, No. 12, pp. 1295-1307, December 1998.

[18.] Info Security Magazine, *Biometrics Technology: Making Moves in the Security Gace,* pp. 28-34 Volume 12 #3 March 2002.

[19] International Biometrics Group, (2002). *Facial Scan Technology: How it Works,* Tech Reports.

[20.] Jain.A,(2007):*Fingerprintmatching,* http://www.pims. math. ca/ industrial /2002/mitacsagm/jain/, January 2007.

[21] Jain A.K. and Arun R. (2002): *Learning user-specific parameters in a Multibiometric system,* Dept. of Computer Science and Engineering – Michgan State University, Proceedings International Conference on Image Processing(ICIP),2002.URL:http//biometrics.cse.msu.edu/JainRossalICIP2002 .pdg.

[22] Jain, A.K, Prabhaka, S and Maltoni, D (1999): *Biometrics: Personnel Identification in Networked Society,* Kluwer Academi Publishers, USA.

[23] Jain, A.K. Flynn, P.J and Ross, A (2007): *Handbook on Biometrics,* Springer-Verlag, New York.

[24] Jain. A and S. Pankanti, (2007): *Fingerprint Classification and Matching,* http://www.research.ibm.com/ecvg/pubs/sharat-handbook.pdf, January 2007.

[25] Jiang X. and W. Yua, (2000): *Fingerprint Minutiae Matching based on the Local And Globa Structures,* 15th International Conference on Pattern Recognition (ICPR'00). Vol. 2. 2000. Pp. 1038-1401.

[26] Liu, S and Silverman, M (2000): *A practical Guide to Biometric Security Technology,* IT Professional, IEEE Computer Society Magazine 3 Feb (01) p. 4.

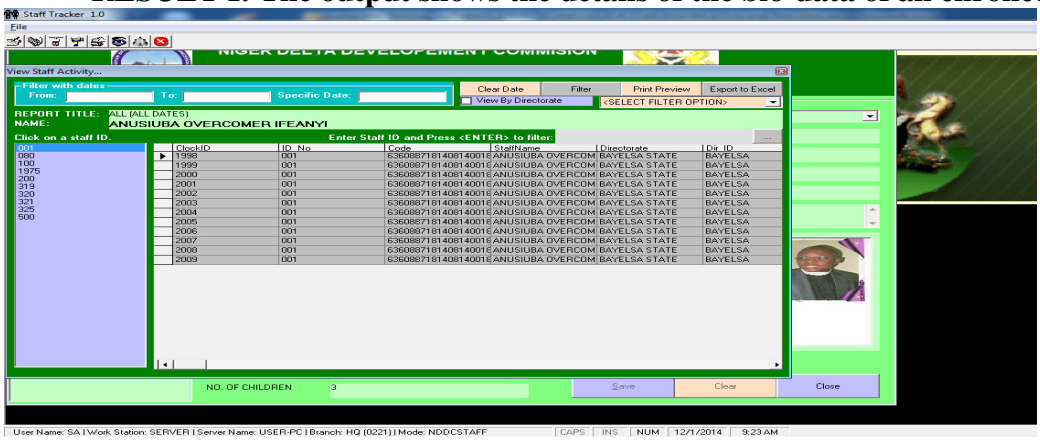
[27] Liu, S.Z and Jain, A.K. (2005): *Handbook of Face Recognition,* Springer, New York.

[28] Maltoni, D., Maio, D., Jain, A.K and Prabhakar, S (2003): *Handbook of Fingerprint Recognition,* Springer, New York.

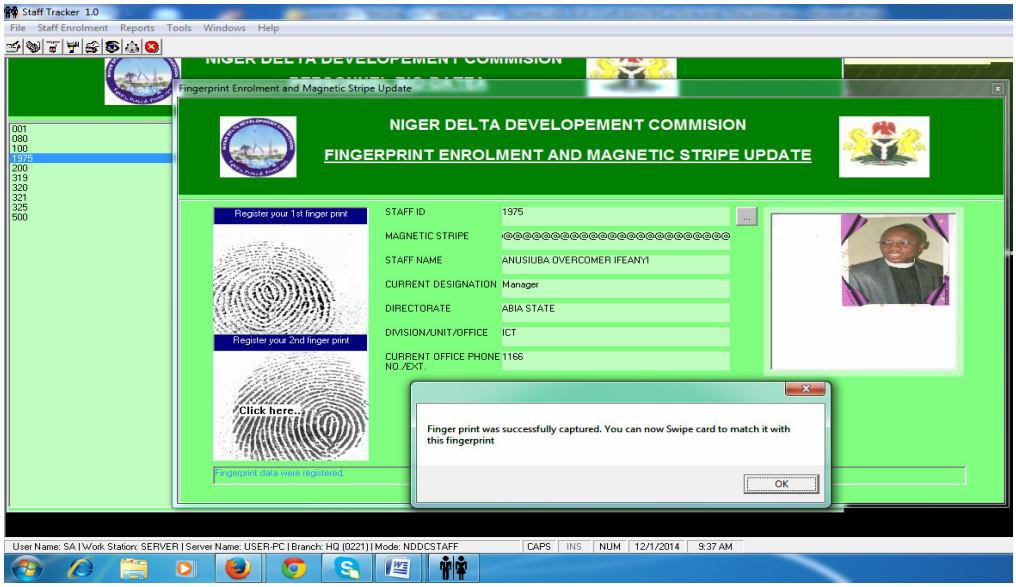
[29] Osuagwu, O.E, Kembe, et.al (2007): *Blocking Credit Card Theft through Biometric Authentication System,* NCS 21st National Conference Proceedings 2007, Vol 18 pp 24, 25.

APPENDIX
THE OUTPUT/RESULTS

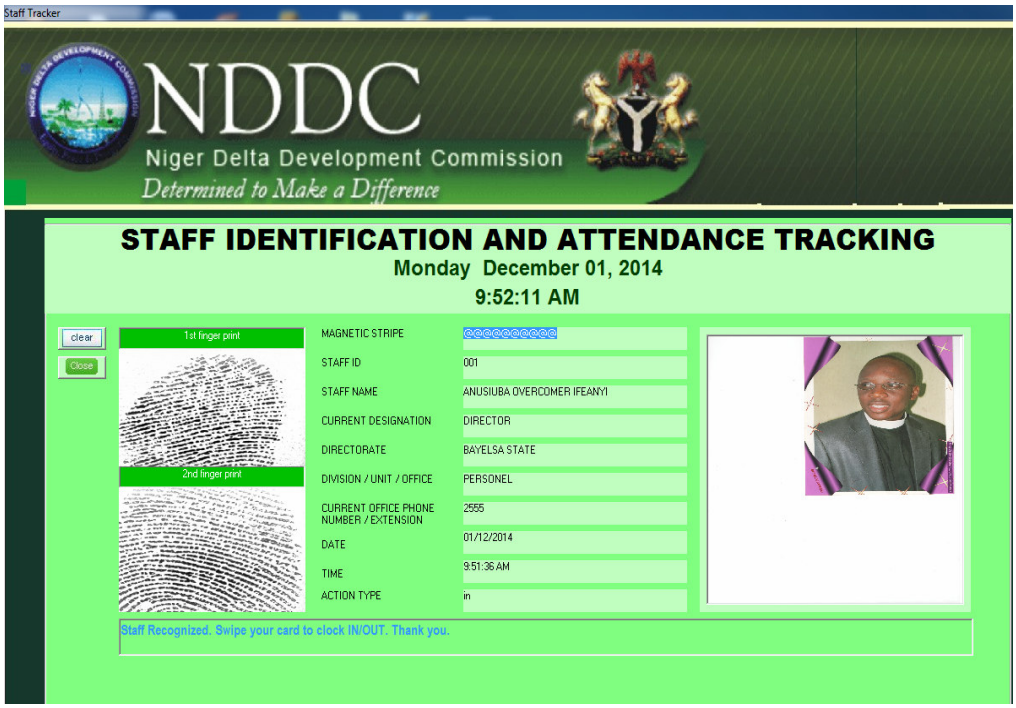
RESULT I: The output shows the details of the bio-data of an enrolled staff



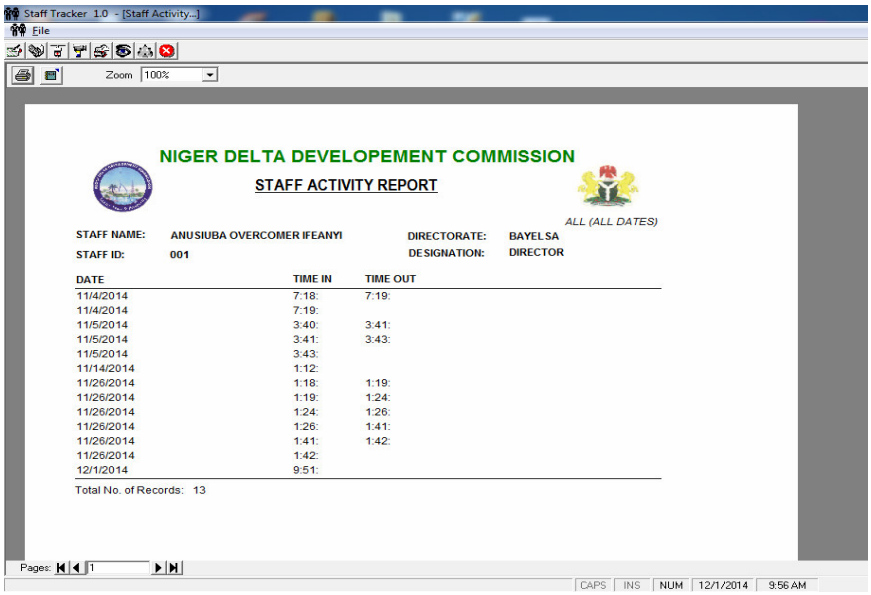
RESULT 2: The output showing the activities of a staff the log in and out details



RESULT 3: The output of the captured fingerprint and magnetic stripes for staff enrollment



RESULT 4: The output of the Identification and Attendance Tracking



RESULT 5: The output of the Staff activity and Attendance Tracking