KWAME NKRUMAH UNIVERSITY OF SCIENCE AND TECHNOLOGY, KUMASI

COLLEGE OF SCIENCE

FACULTY OF PHYSICAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

IMPROVING SECURITY LEVELS IN AUTOMATIC TELLER MACHINES (ATM) USING MULTIFACTOR AUTHENTICATION

A Dissertation Presented to the Kwame Nkrumah University of Science and Technology, Faculty of Physical Sciences, in Partial Fulfilment of the Requirements for the Award of the Master of Science in Information Technology

Submitted By:

NTI ISAAC KOFI

September, 2016

CERTIFICATION

I declare that this thesis work is my own work. It is being submitted for the degree of Master of Science in Information Technology at the Kwame Nkrumah University of Science and Technology (KNUST), Kumasi. It has not been submitted for any degree or examination in any other University. Nevertheless, it is probable for readers of this work to detect some errors or omissions. In view of this, I accordingly accept being responsible in that regard.

NTI Isaac Kofi

Index No.: PG8967313	……..	…….
(Candidate)	Signed	Date

Certified by:

Mr. Frimpong Twum	……..	…….
(Supervisor)	Signed	Date

Certified by:	……..	…….
Dr. James Benjamin Hayfron-Acquah	Signed	Date
(Head of Department)		

DEDICATION

This research work is dedicated to Nicolasa & Isabella (my daughters), Bridgitte (my wife) Mrs Mary Nti (my mother), Elvis Nti and all my siblings.

ACKNOWLEDGEMENTS

Firstly, I give all my praises and extreme thanks to God Almighty for how far He has brought me faithfully in life.

Secondly, my sincere thanks to my supervisor, Mr. Frimpong Twum, for his time, dedication, wise guidance, supervision and above all, for introducing me to the world of research.
His encouragement and suggestions made me more confident to overcome many challenges during the conduct of this research. His readiness for consultation at all times, educative comments, concern and assistance have been instrumental.

My next thanks to all non-teaching and teaching staff of the Electrical and Electronic Engineering Department of Sunyani Polytechnic for the constant encouragement and support they offered me during the conduct of this research.

Also, my sincere thanks to my parent (Mary Nti and Fred Kofi Nti), my lovely wife (Bridgitte Owusu-Boadu) and Mr. Kwasi Antwi-Boasiako for their prayer, love, moral and financial supports.

Finally, to all my classmates who offered me all sorts of help in the course of this research, I am saying thank you.

ABSTRACT

A wide variety of systems need reliable personal recognition systems to either authorize or determine the identity of an individual demanding their services. The goal of such systems is to warrant that the rendered services are accessed only by a genuine user and no one else.

In the absence of robust personal recognition schemes, these systems are vulnerable to the deceits of an impostor. The ATM has suffered a lot over the years against PIN theft and other associated ATM frauds. In this research is proposed a fingerprint and PIN based authentication arrangement to enhance the security and safety of the ATM and its users. The proposed system demonstrates a three tier design structure. The first tier is the verification module, which concentrates on the enrollment phase, enhancement phase, feature extraction and matching of the fingerprints. The second tier is the database end which acts as a storehouse for storing the fingerprints of all ATM users' preregistered as templates. The last tier presents a system platform to relate banking transactions such as balance enquiries, mini statement and withdrawal. The system is developed to run on Microsoft windows Xp or higher and all systems with .NET framework employing C# programming language, Microsoft Visio studio 2010 and SQL server 2008. The simulated results showed 96% accuracy, the simulation overlooked the absence of a cash tray. The findings of this research will be meaningful to the Bank of Ghana (BoG) and the Ghana Association of Bankers (GAB).

TABLE OF CONTENTS

CERTIFICATION ii

DEDICATION iii

ACKNOWLEDGEMENTS iv

ABSTRACT v

TABLE OF CONTENTS vi

LIST OF FIGURES x

LIST OF TABLES xii

LIST OF ABBREVIATIONS xiii

Chapter 1 .....

1 GENERAL INTRODUCTION

..... 1

1.1 Background to the Research 1

1.2 Statement of the problem 6

1.3 Aim of Research 7

1.3.1 Specific Objective of the Research Study 8

1.4 Research Questions 8

1.6 Significance of the Research 8

1.7 Scope of Work 9
1.8 Structure of Thesis 9

Chapter 2 .....

10 REVIEW OF LITERATURE.....

10

2.0 Introduction 10

2.1 Automated Teller Machines (ATM) 10

2.1.1 The Benefits of ATMs 11

2.1.2 How ATM Works 12

2.1.3 Internal Structure of ATM 14

2.1.4 Interactive components of ATM 16

2.2 Security Level at ATM systems and Its Developmental Trends 17

2.2.1 Common ATM Frauds 18

2.3 An Overview of ATM Authentication Methods 26

2.3.1 Knowledge based authentication 26

2.3.1.1 Flaws associated with Knowledge based authentication 27

2.3.2 Token based authentication..... 28

2.3.3 Biometric based authentication 29

2.4 Related Works on ATM Security 31

2.4.1 Why additional security for ATM..... 31

2.4.2 Research work on ATM security improvement 35

2.5 Why fingerprint 43
2.6 Conclusion 44

Chapter 3 .....

46 METHODOLOGY

..... 46

3.0 Introduction 46

3.1 Materials Used..... 46

3.1.1 Fingerprint Image Scanner 46

3.1.2 Software Development tool 47

3.2 Methods Used 48

3.2.1 Design Criteria and Concept 48

3.2.2 Fingerprint Identification Algorithm 53

3.2.3 Steps for Fingerprint Image Processing 55

3.2.4 System Design Approach 64

3.2.5 Software Modules Design 66

Chapter 4 .....

74 RESULTS AND DISCUSSIONS .....

74

4.0 Introduction 74

4.1 Experimental Analysis 74

4.3 Software Testing 75

4.3.1 Intra-class variations test..... 77

4.3.2 False Rejection and False Acceptance Rate 79

4.4 Conclusion 84

Chapter 5 .....
85

CONCLUSIONS AND RECOMMENDATIONS 85

5.0 Introduction 85

5.1 Conclusion 85

5.2 Recommendation 86

REFERENCES .....
88

APPENDIX A 96

LIST OF FIGURES

Figure 2.1 The Interconnection between the ATM systems. (Source: (Agarwal, 2010)) 13

Figure 2.2 The Internal Structure of the ATM. (Source: (Agarwal, 2010) 14

Figure 2.3 The Upper and Lower Units of an ATM. (Agarwal, 2010)..... 15

Figure 2.4 Graphical Interface of an ATM 16

Figure 2.5 ATM Skimming Device. (Krebs, 2010) 19

Figure 2.6 ATM Card Trapping. Source (Agarwal, 2010) 20

Figure 2.7 How Phishing Attack Works. Source: cccindy.com 22

Figure 2.8 Shoulder Surfing. (Source: www.crazylearner.org) 23

Figure 2.9 Cash is trapped by the false withdrawal shutter. Source: (Agarwal, 2010) 24

Figure 2.10 Eavesdropping 25

Figure 2.11 Categories of Biometrics. 30

Figure 2.12 ATM related attacks. Source: (Onyesolu & Ezeani, 2012) 34

Figure 2.13 ATM Related attacks by total reported losses in Europe. Source: (Onyesolu & Ezeani, 2012) 34

Figure 2.14 Comparative survey of fingerprint with other biometric features in 2004. Source: (Iwasokun, et al., 2012)..... 43

Figure 3.1 A Fingerprint Scanner 47

Figure 3.2 Conceptual Design of Proposed ATM Security Structure. 49

Figure 3.3 Flow Chart of Proposed System 50

Figure 3.4 Block Diagram of User Fingerprint enrollment 51

Figure 3.5 A flow chart for fingerprint enrollment process 54
Figure 3.6 Authentication Process Flow Chart 55

Figure 3.7 The Conceptual Diagram of the Fingerprint Enhancement Algorithm 56

Figure 3.8 Ridges and Valleys on a Fingerprint Image 57

Figure 3.9 A Fingerprint Image and its Foreground 57

Figure 3.10 The Orientation of a Ridge Pixel on a Fingerprint. 60

Figure 3.11 Waterfall model 64

Figure 3.12 Use Case Diagram for Proposed ATM Multifactor Authentication Module 66

Figure 3.13 Code Map and Relations 67

Figure 3.14 Detail Code Elements and Relation 68

Figure 3.15 Module for Customer Enrollment onto the Fingerprint System from bank hall 69

Figure 3.16 Module for Customer Enrollment unto the Fingerprint System from ATM 70

Figure 3.17 Welcome Screen for Customer at ATM centre 71

Figure 3.18 PIN Authentication Module 72

Figure 3.19 Proposed Finger Print Verification Module Interface 73

Figure 4.1 Same PIN for two or More ATM Card 75

Figure 4.2 Intra-Class Variations Matching Score Distribution 78

Figure 4.3 False Rejection Rate Score 80

Figure 4.4 False Acceptance Test 81

Figure 4.5 ROC Curve for Experiment on Dataset (A) 82

LIST OF TABLES

Table 1.1 Fraud Type by Percentage 4

Table 4.1 The Average matching time for all three datasets 83

LIST OF ABBREVIATIONS

ATM	Automatic Teller Machine
AFIS	Automatic Fingerprint Identification Systems
BoG	Bank of Ghana
DNA	Deoxyribonucleic Acid
EAST	European ATM Security Team
EMV	Europay, MasterCard and Visa
FAR	False Acceptance Rate
FTE	Failure-to-Enroll Rate
FMR	False Match Rate (FMR
FNMR	False No match Rate
FRR	False Rejection Rate
GAR	Genuine Acceptance Rate
GCB	Ghana Commercial Bank
GAB	Ghana Association of Bankers
HSBC	Shanghai and Hong Kong corporation
HSM	Hardware Security Module
ISO	International Organization for Standardization

ISP	Internet Service Provider
IBG	International Biometric Group
IP	Internet Protocol
LAN	Local Area Network
LSM	Least Square Mean
MSSQL	Microsoft Structured Query Language
OTP	One-Time Password
PIN	Personal Identification Number
RDBMS	Relational Database Management System
SDK	Software Development Kit
SDLC	System Development Life Cycle
TCP	Transmission Control Protocol
TER	Total Error Rate

Chapter 1

GENERAL INTRODUCTION

1.1 Background to the Research

The advancement of payment system in the modern world has gone passed cash to cheques, and then to payment cards such as credit cards and debit cards (Batiz-Lazo & Barrie, 2005). Automatic Teller Machine ATM is a terminal installed by banks or other financial institution that enables customers to perform service, like cash withdrawal or cash deposit, balance enquiry, request for bank statements, and money transfer from one account to the other. Some modern ATMs are equipped with mobile money transaction. ATMs are basically independent banking workstations which aims at providing a faster and expedient services to customers (Rasiah, 2010). Barclays bank introduced the first ever ATM in 1967, in its Hendson branch in London, which could dispense a fixed amount of cash when a user inserted a special coded card and since then, ATM has become smaller, faster and easier (Das & Jhunu, 2011). Among all departments in a financial institution, the ATM has been considered as one of the important components of electronic banking infrastructure.

The main benefit of the ATM is its ability to provide a 24hours service daily to customers and users, making the ATM an integral part of our everyday life. Nowadays, ATMs' are employed in various scenarios such as ticket vending machines, quick check-in kiosks and self-service gas stations (Luca, 2011).

ATMs are not only sited at banks, but also a lot of schools and businesses nowadays installed ATM on their premises for customer convenience and more revenue. A global ATM market forecast

research lead by Retail Banking Research Limited (Mohammed, 2011) shows that there are 1.8 million ATMs deployed around the world and the figure was forecast to reach 2.5 million by 2013. ATMs cards authentication methods have little changed since their introduction in the 1960's. The security limitations of ATM are mostly derived from the security pitfalls of the magnetic media. The data on the magnetic stripe are usually coded using two or three tracks, because, it is not difficult or expensive to have the equipment to encode magnetic stripes. The standard covering this area is International Organization for Standardization (ISO) 7811 and the technique for writing of the tracks is known as Friend-to-friend (F/2F). Thankfully, magnetic stripe feebleness has been partly addressed by the introduction of Europay, MasterCard and Visa (EMV) smartcards. Normally, the authentication design involves a trusted hardware device (ATM card or token). The Personal Identification Number (PIN) of the card holder's is usually the only means to attest the identity of the user; this approach is vulnerable to misplacement, unauthorized access, card swallowing, forgetfulness and others (Das & Jhunu, 2011), (Akinyemi, et al., 2010).

Despite the numerous cautions given to the card user, many people continue to choose easily guessed passwords and PINs such as phone numbers, birthdays and social security numbers.

However, due to the limitations of this design, an intruder in possession of a user's card can discover the user's PIN with password prediction or guessing (brute force) attack. For instance, in a typical four digits PIN, one in every 10,000 users will have the same number. In spite of all security measures in place, cases of ATM crimes continue to occur globally. A current figure by European ATM Security Team (EAST) affirms that there is a rise in ATM fraud "trend", especially of skimming attacks. An upsurge of 24 % in skimming attacks at European ATMs, matched to the first half of 2009, is reported for the first half of 2010 in the ATM Crime Report (Gunn, 2010).

In situations where a user has two or more ATM cards, all PINs needs to be memorized by the user. This can easily lead to the user initiating security problems (Adams & Sasse, 1999), thus a card

holder or user may decide to write down the authentication token, or use the same authentication token (PIN) across different services or use authentication token (words) that can be found in dictionaries. A notable example of this was shown by Klein, who could crack 25% of 14,000 passwords using a dictionary attack with only 86,000 words (Jermyn, et al., 1999) and (Luca, 2011). This leads to the saying that the user is often referred to as the 'weakest link' in the security chain (Luca, 2011).

With the introduction of internet technology in recent years, the internet communication is exposed to unwanted people giving them access to pose different kinds of attacks on ATM System. Figure 1-1 shows a comparative survey of ATM attack (Lavanya & Raju, 2013).

Some of the threats posed to the ATM are like:

- Eavesdropping
- Spoofing
- Skimming Attacks
- Card Trapping
- PIN Cracking
- Phishing Attacks
- ATM Malware
- ATM hacking

Table 1.1 Fraud Type by Percentage

Fraud Type By Percentage	Yearly Average
Counterfeit	30.59%
Stolen	26.77%
Lost	14.53%
Card Not Present	12.82%
Fraudulent Application	11.43%
Account Takeover	3.72%
Multiple Sales Drafts	0.08%
Not Received	0.06%

(Source: (Tedder, 2009))

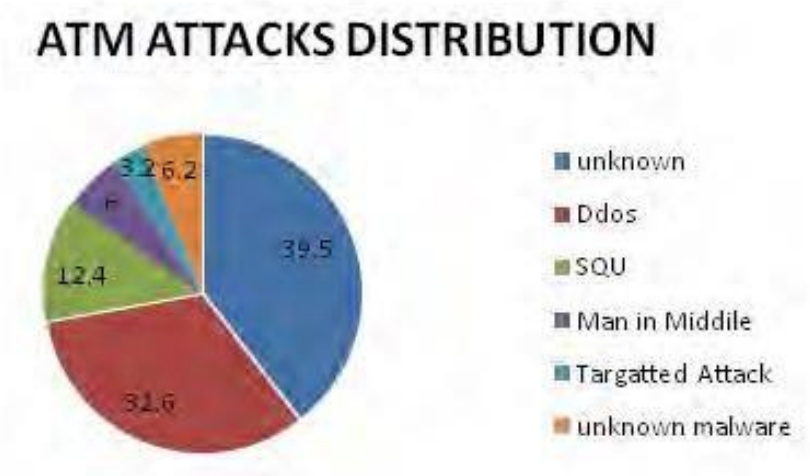

Figure 1-1 Comparative survey of ATM attacks. (Source: **(Lavanya & Raju, 2013)**)

According to the European ATM Security (EAST), a total of 1,459 ATMs were raided all over Europe in the first half of 2009, totaling 4.5 crimes or attacks annually for every 1,000 ATMs.

And also 26 ATMs were robbed starting November 2007 to November 2008, totaling 18 crimes per thousand ATMs out of 1,471 ATMs in Lithuania (Dare, 2011).

In 2013 Australia recorded growth from 43.6 cents in 2012 to 48.7 cents for every $ 1,000 spent; this is against an increase of 4% to $624 billion on the total amount spent by Australians. While card not present fraud increased from 45% in 2008 to 72% in 2013 in Australia. At the same time, UK saw an increase in card fraud rates from 71 pence to 74 pence in every £1,000 spent. Cardnot-present fraud on UK cards increased from £246.0 million to £301.1 million (APCA, 2014).

In 2013 Ghana Commercial Bank (GCB) confirms money theft from an ATM of about GH¢3 million (Obour, 2013) and a worldwide gang of criminals stole $45 million in a matter of hours by hacking their way into a database of prepaid debit cards and then draining cash machines around the globe (Modernghana, 2013). ATM's crime has become a nationwide epidemic which faces both customers and bank operators, as well (Richard & Alemayehu, 2006) cited by (Das & Jhunu, 2011). The security breaches in the ATM system have contributed to the less patronage and rejection of the ATM, by some customers of various banks (Ndife, et al., 2013).

The introduction of biometric authentication technology will eliminate entirely or help reduce this problem since a person's biometric data is undeniably connected to its owner; a person bio data is nontransferable and unique for every individual. A biometric system has the ability to compare scanned bio-data to recorded bio-data in local or central storage system.

This thesis proposed a multifactor framework authentication for ATM application. The framework comprises of a unit for the traditional PIN and a fingerprint enrolment database and verification.

The verification section consists of, the normal PIN and a fingerprint quality improvement, feature removal and matching sub-modules, which are all supported by suitable mathematical formulas.

The application will be designed for Microsoft Windows Xp or higher as operational platform, Microsoft SQL server as backend and C# served as the front-end engine.

1.2 Statement of the problem

The traditional authentication of ATMs is by the use of secret passwords or PIN (personal identification chip and PIN). There are major security problems associated with these authentication mechanisms. The use of a four-digit PIN as authentication mechanism is very easy to understand, memorized and permits fast communication (Luca, 2011), but it is less secure, since there is no protection mechanism built into the authentication process (besides showing asterisks on the screen instead of the real input) (Luca, 2011). Thus the "secret token" (PIN) is input in plain view of anyone around. As commonly known practice the input of PIN takes place in a public domain, in the view of anyone closer to the ATM and this can easily be spied on or be manipulated. This problem has been emphasized by a huge number of reported ATM frauds every year all over the continent. Due to the virtue of the ATM giving direct access to a user's bank account, thus savings or current, ATMs are the number one target for criminal activities.

In 2009, there were 2,058 reported manipulations of ATMs in Germany, which led to more than 100,000 users becoming victim to ATM frauds, resulting in a 20% compared to 2008 and this trend continues in 2010 (Bianchi, et al., 2010), and in 2013 Ghana recorded its biggest ATM fraud (Obour, 2013). These statistics only include attacks that were due to direct manipulations of the ATM, called "skimming" attacks. Shoulder surfing, a very common attack, is not even covered by these statistics. Again, the positioning of the ATMs in the public domain makes such a simple attack possible and so effective.

Another problem that comes with the use of standard PIN or password is the users themselves being a threat to the system and compromising its security. In the field of usable privacy and security, a sub-field of human-computer interaction (HCI), the common believe is that teaching the users to behave more securely, e.g. by using punishment, will not solve this problem as already stated by Adams and Sasse (Luca, 2011). The best solution seems to be considering the users when designing authentication mechanisms ("user-centred design").

The increase rate of break-in reports on traditional ATM authentication (PIN and Password), has called for greater security measure for access to personal and sensitive data (Han, et al., 2006) As a result of the weaknesses of PIN and password in their current form, research in this area often focuses on how to make authentication mechanisms more secure.

1.3 Aim of Research

The aim of this research is to identify the security weakness associated with PIN authentication and develop a multifactor (PIN and Fingerprint) based authentication system for ATM's in order to reduce frauds associated with the use of ATM

1.3.1 Specific Objective of the Research Study

The specific objectives of this research are:

1. To examine security challenges of the ATM system.

2. To establish if the use of a multifactor authentication mechanism can address these challenges.
3. To proposed a multifactor authentication model for dealing with modern ATM's security challenges and examine its performance.

1.4 Research Questions

The study seeks to address the following research questions;

1. What security challenge(s) confronts modern ATM system usage?
2. How can multifactor authentication be used to address security challenges confronting the ATM system?
3. Can a proposed multifactor authentication security software by this study alleviates modern ATM security challenges?

1.6 Significance of the Research

The significance of this study is summarized as follows:

- With the introduction of the fingerprint authentication in addition to the normal PIN authentication will eliminate an ATM card fraud total from the scene.
- More people will have confidence and trust in Electronic bank, giving more revenues to the banking industries.
- The result obtains can serve as a reference material to researches researching into ATM security.

1.7 Scope of Work

This thesis is sentence on the development of a Fingerprint and a PIN authentication mechanism to improve security levels at the ATM system.

1.8 Structure of Thesis

This thesis is structured into five chapter staring with the general introduction as chapter one. Chapter two captures literature review of previous and related works.

Chapter three outlines propose possible solutions that have been developed in the scope of this work and contribution made in improving authentication mechanisms at ATM systems.

Chapter four focuses on results and discussion of the research.

Chapter five rounds up with conclusions and recommendations.

Chapter 2

REVIEW OF LITERATURE

2.0 Introduction

This chapter serves as the review of literature to this research, it first present definition of ATM system; its configuration, basic components and its authentication levels. The chapter further looks at terminologies in relation to ATM, briefly discourses of different security breaches in ATM systems, and authentication methods. Lastly, this chapter will conclude with a review of some conventional authentication levels and techniques in ATM security, along with their strength and weakness and an eventual summary.

2.1 Automated Teller Machines (ATM)

Automated Teller Machine shortens (ATM), may be described as an electronic machine that permit an account holder of a bank to perform some transactions on their own accounts (current, savings and etc.). The ATM is said to be inverted by John Shepherd-Barron in June 1967 in the United Kingdom at Barclays bank in Enfield. The First public appearance of the Automated Teller Machine was in 1987 installed by Shanghai and Hong Kong corporation (HSBC) based in India. ATMs were then installed in most banking halls and premises of Citi bank and Indian bank (Gazal & Ranjeet, 2014).

In other words, an ATM system can be said to be a real-time front terminal of automatic teller services with the support of a centralized accounting database and a central bank server.

According to (Jegede, 2014) an Automatic Teller Machine is a combination of a computer terminal, a record keeping system, and a cash vault, in one unit, which allow bank customers to access a banking institution accounting system with a smart or plastic card containing a Personal Identification Number (PIN) or by hitting a distinct code number into a computer terminal linked to the financial firm's computerized records 24 hours a day.

2.1.1 The Benefits of ATMs

The Introduction of the ATM in the banking industry, has done great good to both the customers and the bankers. With the ATM in place customer can withdraw cash from the ATM without joining long queues in the banking hall and in some cases customers can perform cash deposit into their respective accounts directly from the ATM (Omari, 2012).

The current introduction of interbank transaction has also added more value to the ATM transaction, a customer with VISA card can withdraw cash not from only his mother bank ATM, but any ATM that accepts VISA transaction. Current ATM's are equipped with MTN and Airtel mobile money transaction, making it easier for customers and clients to have quick access to their money at ease and anytime.

The ATM introduction into the banking industry has also reduced the pressure on banking staff, because the number of customers that would have gone inside the banking hall to withdraw, deposit, mini statement and balancing checking has reduced considerably. Because customers can perform all these transactions at the ATM terminal.

The introduction of the ATM into the financial firms has brought about a reduce in the volume of paperwork, thus a customer who wishes to use the ATM need not to fill any withdrawal form or cheque book before cash withdrawal can be effected (Omari, 2012). Thus, the advert of technology into the banking industry has open chances for reduction of both paper and people (William, et al., 2005) cited by (Omari, 2012).

It is estimated that, the ATM performs an average of six thousand four hundred (6,400) transactions in a month while a human teller performs four thousand three hundred (4,300) (Rose, 1999) cited by (Jegede, 2014) making the ATM an economical way of acquiring higher

productivity

2.1.2 How ATM Works

The ATM can be said to be a data terminal which comprises of two main inputs and four outlets (outputs), the ATM like all or most devices for communication, communicates by connecting via a host processor. The host (processor) being an Internet Service Provider (ISP), which became the gateway through which all the various ATM networks are made available to the cardholder (the person wanting withdrawal or deposit cash) (Agarwal, 2010).

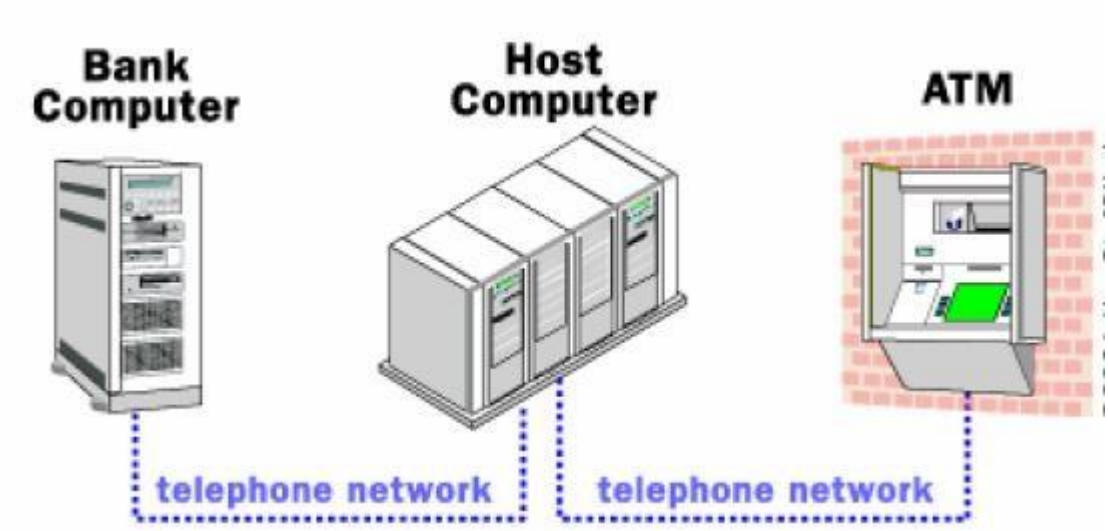

Figure 2.1 The Interconnection between the ATM systems. (Source: (Agarwal, 2010))

Most processors employed in ATM servers can support either leased-line or dial-up machines (ATMs). With Leased-line machines, they make direct contact with the host via a four-wire, an out-and-out telephone line and point-to-point. Dial-up ATMs connect to the host processor through an ordinary phone line by means of a modem with a toll-free number, or through an Internet service provider using a local access number dialed by the modem (Agarwal, 2010).

The ATM uses **A**synchronous **T**ransfer **M**ode, network technology for fixed data size transfer in cells or packets. This cell ATM is smaller enhanced with technologies that gives the ATM the ability to transmit audio, video, and computer data over the same network, with assurance that no single type of data hangs onto the line. Some school of thought argues that ATM holds the answer to the internet bandwidth problem, whiles others do not believe in that.

The automatic teller machine (ATM) generates a fixed route or channel, between two points whenever data transfer initiates. This mode of transmission differs from TCP/IP transmission where messages are distributed in packets, where each packet may take a different route from source to destination and reassembly at destination. This process of ATM transmission makes it simple and convenient to track and bill data usage across ATM networks, but it makes it less flexible to sudden surges in network traffic (Gazal & Ranjeet, 2014).

2.1.3 Internal Structure of ATM

The ATM can be divided into two different parts:

- Upper unit
- Lower unit

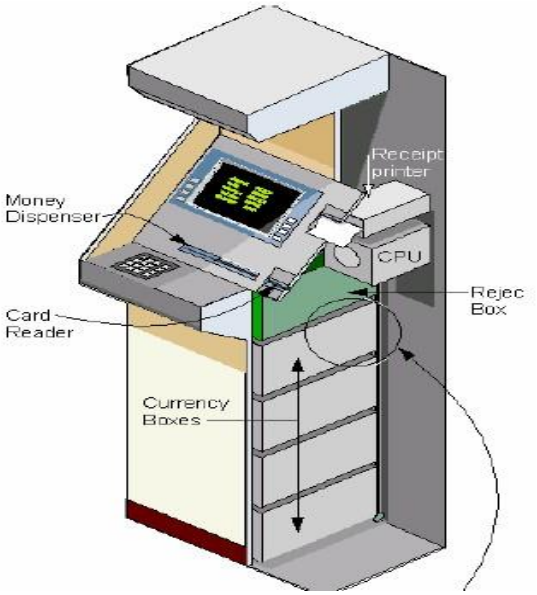

Figure 2.2 The Internal Structure of the ATM. (Source: (Agarwal, 2010)

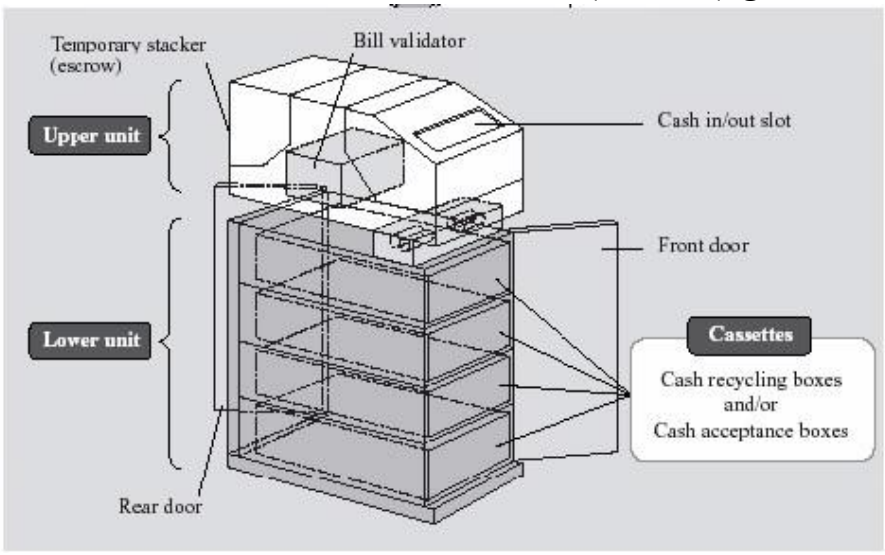

Figure 2.3 The Upper and Lower Units of an ATM. (Agarwal, 2010)

The upper unit houses the CPU and the processes that validate customer details by connecting to the customer's bank computer or server, when a customer enters his or her ATM card. The ATM has few layered boxes called currency boxes or cassettes in the lower unit of it, where currencies are kept for withdrawal or for keeping the deposited money. A sensing mechanism (rubber roller) is present to ensure that a single banknote moves at a time, and also to ensure that the bills don't

stick together when cash is being dispensed. A receipt printer is attached to the system to print current statistics of the cardholder's account transaction (Agarwal, 2010).

2.1.4 Interactive components of ATM

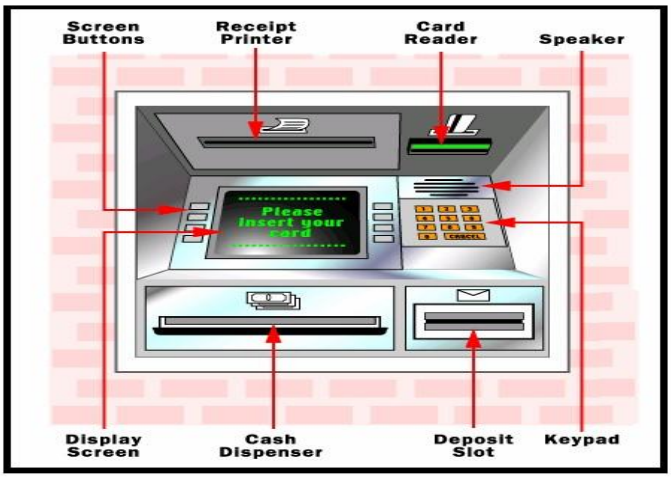

Figure 2.4 Graphical Interface of an ATM

Keypad: The alphanumeric keypad serves as an input device to the ATM, from the customer's viewpoint, that enable customers for PIN code input, withdrawal/deposits amount input and PIN change (Agarwal, 2010).

Card Reader: It is an open slot on the ATM where customers insert their ATM card in, when the ATM screen prints "Please insert your card" (Agarwal, 2010).

Display Screen: This is a normal visual display unit, attach to the ATM for display information and instruction as a message to the customer (Agarwal, 2010), thus it serves as a platform for the ATM to talk to its clients.

Cash Dispenser: This slot is responsible for giving out the withdrawal money.

Screen Buttons: Users of ATM use the screen button for choosing option they are displayed on the screen during an ATM transaction.

Speaker: The function of the speaker is to provide audio feedback to the ATM user.

Deposit slot: This is an additional slot fitted on modern ATM in addition to the cash dispersion slot, which enable customer to perform cash deposit into their own respective accounts from the ATM terminal (Agarwal, 2010).

2.2 Security Level at ATM systems and Its Developmental Trends

Computers have practically taken over all of our major record keeping functions and system nowadays. Lately, personal computers have made it less expensive to automate many office functions and also share data across a wide area networked computer. Computerization comes with countless advantages with automated systems, but however, introduces new risks. Firms, Organizations and Associations such as telecommunications, power distribution, national defence, law enforcement; financial services, government services and emergency service that employs computer systems are exposed to enormous forms of security threats, due to interconnectivity. Thus to say security is associated with threat, vulnerability and risk (Bhosale & Sawant, 2012). Lalzirtira (2013) emphasized that in human computer interaction there are three major sections that are of importance, namely authentication, security operation and secure system

Financial institutions that renders internet banking or electronic banking (e-banking) service for its customers should have effective and reliable methods to authenticate customers. A more effective and secured authentication method is necessary for compliance and a requirement to safeguard customer information (Bhosale & Sawant, 2012) to prevent money laundering and terrorist financing, (Roth, et al., 2004) to reduce fraud, to impede identity theft, and to encourage the legal enforceability of electronic agreements and transactions. The threats of engaging in business with unapproved or incorrectly identified persons in an internet banking environment can or may lead to financial loss and damage of reputation through fraud, disclosure of customer information, corruption of data, or unenforceable agreements.

2.2.1 Common ATM Frauds

The wide utilization of internet technology in recent years makes it a necessity to improve and increase the security level at the ATM, because the internet communication is exposed to unwanted people, allowing them to do different kinds of attacks on ATM System (Ndife, et al., 2013). There are numerous password attacks on ATM, but in this section of this research few are described, so that the user of the ATM can understand and beware of unauthorized access or password attacks. Basically, there are three main attacks that ATMs are subject to, namely;

i. *Physical attack*: Brute force attack, thus applying mechanical force on the ATM machine, with the intention of getting access to cash within the safe.
ii. *ATM Fraud:* Bank card information theft, using an unauthorized means to get access to the customer's information stored on the ATM card.
iii. *Software and network attack:* Theft of sensitive information or controlling ATM operations from a remote distance or automatically.

These basic three ATM attacks can be further broken into;

- Skimming Attacks
- PIN Cracking ➢ Phishing Attacks
- Shoulder Surfing:
- Card Trapping
- Cash Trapping
- ATM Malware

2.2.1.1 Skimming Attacks

The skimming attack is the most common attack in ATM transaction. In this attack, lawbreakers take advantage of technology to make fake ATM cards by using a skimmer (a card swipe device that reads the information on ATM card). This device looks like a handheld credit card scanner and is often clipped in close proximity to or over the top of an ATM's factory installed card reader (Mandal, 2013). When a skimmer is removed from the ATM, it allows the download of personal data belonging to everyone or customers who used the ATM whiles the skimmer was in place. 200 ATM card information can be stored on single skimmer (Krebs, 2010).

According to Rick Doten, the annual losses from ATM totaled about $1 billion in 2008, or approximately about $350,000 every day from the U.S. Secret Service estimation, Card skimming accounts for more than 80 percent of ATM fraud (Krebs, 2010).

In December 2009 this particular skimmer was attached to the front end of Citibank ATM in Woodland Hills, Calif. (Krebs, 2010)

Figure 2.5 ATM Skimming Device. (Krebs, 2010)

2.2.1.2 Card Trapping

Figure 2.6 ATM Card Trapping. Source **(Agarwal, 2010)**

This involves, placing a device directly over or into the ATM card reader slot, which physically captures the ATM cards when inserted into it. When the user leaves the ATM without his or her card, the card is retrieved by the thieves or hackers. With this attack one ATM card is lost per attack. At every captured card, the hackers or criminals have to withdraw the whole device. Lately a newly card trapping device capable of trapping users' cards for a long time and enhance with the ability of removing trapping cards without removing the trap device have been introduced by ATM fraudsters. The common variant is well-known as the *Lebanese Loop* (Mohammed, 2011).

2.2.1.3 PIN Cracking

Bond & Zielinski made several contributions to attacks on customers' PINs (Bond & Zielinski, 2004). (Berkman & Ostrovsky, 2007) highlighted on one of the most efficient 'PIN cracking' attacks. In their research, they explained how the processing system used by banks is open to manipulation. Some of the attacks target the translate function in switches, and manipulate the functions that permit customers to select their PINs online. In other research, this flaw makes it possible for an attacker to discover PIN codes (Mohammed, 2011). Taking an example, PIN's entered by a customer while withdrawing cash from an ATM, provided they have access to the online PIN verification facility or switching processes. A staff within the bank (insider) can use an existing Hardware Security Module (HSM) to reveal the encrypted PIN codes. In worse case, an insider of a third-party switching provider could attack a bank outside of his terrain or even in another region. Unfortunately, proposals to counter such attacks are almost non-existent other than a few suggestions; for example, maintaining the secrecy (and integrity) of some data elements related to PIN processing (that are considered security insensitive according to current banking standards) such as the 'decimalisation table' and 'PIN Verification Values (PVVs) /Offsets' has been emphasized (Bond & Zielinski, 2004) and (Berkman & Ostrovsky, 2007) cited by (Mohammed, 2011).

2.2.1.4 Phishing Attack

This is an attack on the web, where scammers aim at luring ATM users to provide their card information and PIN details of their bank card. In a typical attack, an attacker uses an email

pretending as a bank and claims that user's account information is inadequate, or users' needs to update their account information to prevent the account from being closed. The user is asked to click on a link and follow the directions provided. The link however is fraudulent and leads the system user to a different website that the attacker has set up which resembles the website of the user's bank.

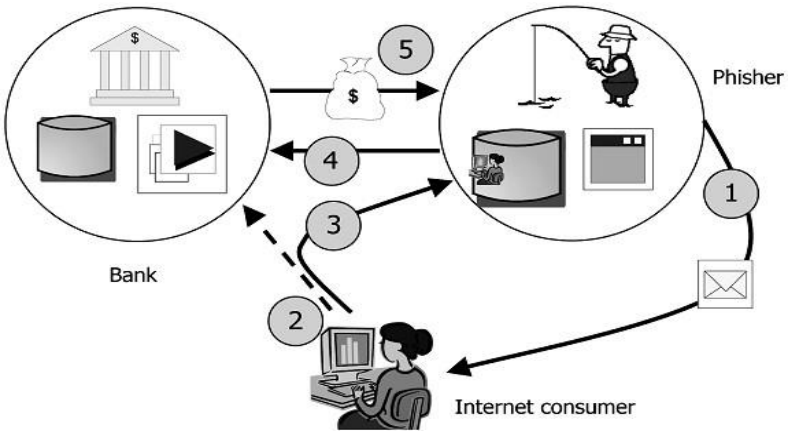

Figure 2.7 How Phishing Attack Works. Source: cccindy.com

The site directs the user to input sensitive information such as card numbers and PINs. The information is collected by the thieves and used to create fraudulent cards. Traditionally, after a successful phishing attack, the criminal would extract the needed information and go into the online account and remove the victim's bank funds (Mohammed, 2011).

2.2.1.5 ATM Malware

This ATM attack requires an insider, such as an ATM technician who has a key to the machine, to install the malware on the ATM operating system or software. Once that has been done, the

attackers could insert a control card into the machine's card reader to trigger the malware, this gives the hacker or attacker an access to control the ATM through a custom interface and the ATM's keypad (Mandal, 2013).

According to (SpiderLabs, 2012), a Trojan family of malware was found to have infected 20 ATMs in Eastern Europe. This malware gave access to criminals to take over the ATM and stole customers' data and cash. This malware then captured the magnetic stripe data and PIN codes from the private memory space of the transaction-processing applications installed on the compromised ATM.

In 2013 a report from a Russian security company reveals that, a new ATM malware was developed by hackers, which infects ATMs and physical registers in order to harvest valuable credit card data. (Wheatley, 2013). The security Week website reported of an ATM malware which was discovered by researchers from Group-IB. Called the "Dump Memory Grabber", this virus is already believed to have stolen data from hundreds of credit and debit cards using major banks in the United States like Capital One, Citibank, Chase and others. (Fahmida, 2013)

2.2.1.6 Shoulder Surfing

Shoulder surfing Attack involves direct observation of ATM's user details by the attacker, such as looking over the shoulder of the card user, to get his/her information.

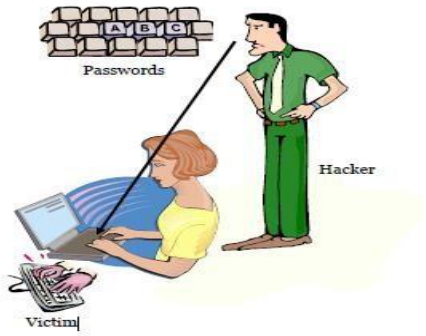

Figure 2.8 Shoulder Surfing. (Source: www.crazylearner.org)

This attack method is very effective in getting ones information in a congested environment, because it's quite easy to stand next to someone or stretch your neck and watch as She/he fill out a form, entering a PIN number at an ATM machine (Mandal, 2013).

Shoulder surfing can also be done from a remote distance with the aid of eyeglasses or other vision enhancing devices. To prevent or minimize shoulder surfing attack, it's advisable to shield the keypad with your body when using an ATM.

2.2.1.7 Cash Trapping

With this attack, the attackers or criminals insert a false withdrawal close up slot. The false slot causes the cash to get stuck within it, whiles a customer is performing a withdrawal transaction on the ATM. The customer will leave the ATM premises, thinking the machine is out of order or may go inside the banking hall or premises to report the incident. The attackers then return to retrieve the money or notes from the ATM.

Figure 2.9 Cash is trapped by the false withdrawal shutter. Source: **(Agarwal, 2010)**

ATM Cash Trapping Cases

On 5th March 2011, the London city police arrested two Romanian of age 23 and 25 within a flat in Harrow. These men were found in possession of cash traps, which have been used to trap customer transactions on various ATM's. (BBC , 2011)

On Thursday, 31 March 2011 two men, ages 23 and 21 were arrested for allegedly trying to steal cash from bank customers by tampering with an ATM in Chingford, using a small plastic strip which causes cash ejected from the ATM to become stuck. (Daniel, 2011)

2.2.1.8 Eavesdropping

Figure 2.10 Eavesdropping

Eavesdropping is the process of secretly listening to the private conversation of others without their consent. Spying on an ATM user and knowing his or her PIN and then obtain his or her card by any faulty means (Mohsin, et al., 2015).

Basic eavesdropping techniques are;

- Viewing victims monitor using binocular through an open window
- Capturing peoples information by installing small cameras whiles the information is being read

ATM Eavesdropping Cases

Global ATM manufacturer NCR Corporation issued an alert about a card reader eavesdropping attacks, which were first identified in Europe in 2014 and are now spreading, potentially posing a risk in the U.S. (Kitten, 2015).

2.3 An Overview of ATM Authentication Methods

Authentication methods can be divided into three main areas, namely:

- Knowledge based authentication
- Token based authentication
- Biometric based authentication

2.3.1 Knowledge based authentication

Knowledge based authentication is the most widely use form of authentication system around the globe, it comprises of the text and picture based authentication mechanism. In this authentication method, a user is presented with a lot of images, for him to identify, the user is given access to the system only when he/she is able to identify the images he/she pre-selected during the registration period or process. Or a user might be asked to provide an alphanumeric PIN to be given access when a PIN is correct. Hence, with knowledge authentication is based on what the user knows.

2.3.1.1 Flaws associated with Knowledge based authentication

The traditional ATM authentication technique consists of text base that uses passwords or Personal Identification Numbers (PINs) and graphic based authentication that uses graphics for authentication. Knowledge based authentication uses secret information, thus when the user provides some information to authenticate himself as a legitimate user, the system processes this information and suggests whether the user is legitimate or not (Khan, 2010).

The numerous disadvantages of the PIN based ATM authorization procedure include ATM card theft, forgetfulness, damages due to bending and card swallowing (Iwasokun & Akinyokun, 2013).

1. It is harder to remember passwords for a long time as time elapses. When a user involves in more than one password based authentication systems, it becomes difficult for the user to distinguish among passwords used for different applications and to correctly remember those passwords. As time passes on, and by using many passwords based applications, forgetfulness of passwords is more probable to occur (Adams & Sasse, 1999).
2. Where a user has more than one account with different passwords, the leakage of one or more of these passwords is just possible.
3. A password that is written down can be seen by others and can be stolen.
4. Passwords invented by customers/people, are derived in a way such that they can be easily be remembered by the user. Example, a word in dictionary, a loved one's name, a telephone number, and a keyboard pattern (i.e. "hjkl"). Unfortunately, a password derived from this approach is considered easier to guess.

This form of authentication is relatively weak because, the same password is used over and over again, giving many opportunities for it to be illicitly captured (Khan, 2010), (Diebold, 2002) .

Once the users' bank card is lost and the password is stolen, the users' account is exposed to attack The possibility of PIN theft by criminals is a major limitation to the operation of ATM (Iwasokun & Akinyokun, 2013)

2.3.2 Token based authentication

A token is a physical device owned by an authorized user of a computer system or service to help him in authentication, thus tokens act as electronic keys. Tokens may be used in place of a password

or in addition to the password, to prove or established that the system user is whom he/she actually claims to be. Most token authentication also employs knowledge based techniques to enhance the security of the system. Example, ATM cards are always used with a PIN. Hence token based authentication can be said to deal with what the user has. Examples of token base authentication are smart cards, key cards and bank cards.

2.3.3 Biometric based authentication

Biometrics is the process of identifying human by their characteristics or traits. Biometric authentication techniques such as iris recognition, face recognition, fingerprints and Palm Print, are rarely adopted widely as a means of authentication. Thus a biometric system is said to be a computer system that implements biometric recognition algorithms (Mudholkar , et al., 2012). This method of authentication provides the highest security level in terms of identification and authentication, but their major setback is the expensive nature and it identification process becomes slow if correct measure are not in place. Biometric based authentication looks at what a person/user is.

2.3.3.1 Biometric techniques classification

Biometric techniques can be classify into two category, namely;

1. Physiological based techniques include fingerprint, facial analysis, retinal analysis, hand geometry, and DNA.
2. Behavior based techniques include key stroke, signature, sweat pores analysis, voice and smell.

Biometric recognition systems built on a behavioural based technique and physiological based techniques are capable of working in two approaches: *identification method*, where a person is identified by a system searching, a huge database of registered or enrolled persons for a match; and *authentication method* where a person's claimed identity is verified by the system from his earlier enrolled pattern.

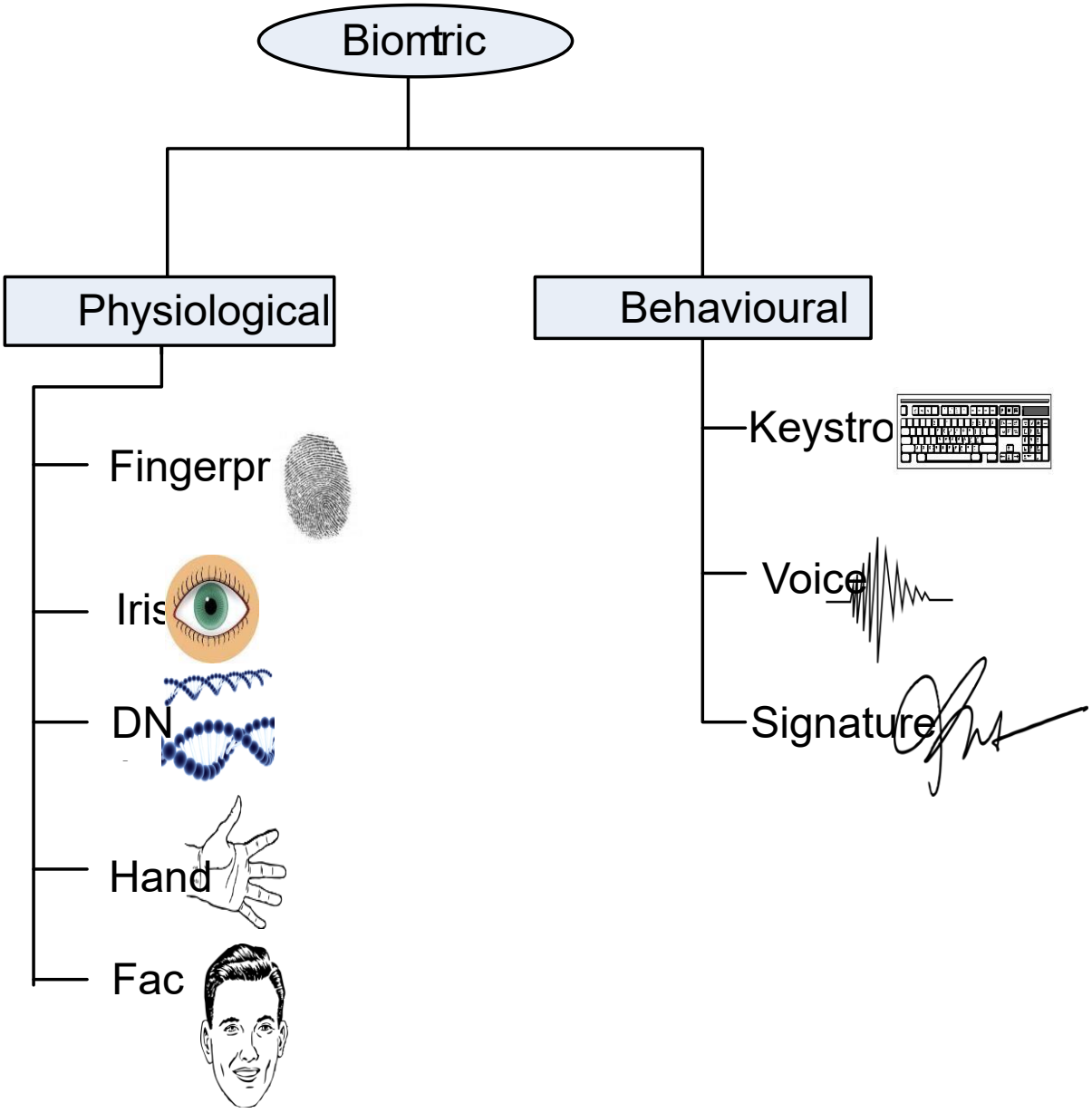

Figure 2.11 Categories of Biometrics.

2.4 Related Works on ATM Security

The traditional password technique (PIN) employed for ATM security is associated with weaknesses and passwords (PINs') that are difficult or hard to crack or guess are often not easy to remember. This causes user to write it down on a piece of paper or somewhere, so that they do not forget it. Studies revealed that humans or users have the ability to remember only a few or a limited number of different passwords, hence user with more password tends to use the same password for different accounts (Lalzirtira, 2013). To defeat the inherent weakness and problem associated with password/username authentication, various alternative authentication methods have been proposed by different researchers and institutions.

2.4.1 Why additional security for ATM

Fraud in ATM service is a growing challenge, and ATM fraud is, and will continue to be a serious challenge to the banking industry. Hence it has become an area of interest, where all contributors seem to be financing significantly to find a solution (Burelli, et al., 2014). With the introduction of several security measures and steps laid down by ATM developers and Banks or financial institutions, ATM crime cases continue to grow globally. ATM crime incidents have been reported in the Americans, Middle East, Asia-Pacific and Africa (Susmita, 2013) and Ghana (Obour, 2013) despite many security measures in place.

In May 2005 an article published in Computerworld revealed how a password cracker software, ran on a network by a security team within a large organisation, in 30 seconds was able to identify approximately 80% of the password used by members of the organisation (Lalzirtira, 2013), and all identify passwords were alphanumeric.

A Japanese bank located in Tokyo reported in 2005 of an ATM crime carried out by a group of criminals that used wireless charge coupled device (CCD) camera recorders to steal hundreds of their customers' detail from ATM outlets. The bank's investigation team revealed that more than 60 ATMs in the metropolitan were under this attack (Hirakawa, 2013).

In 2002 Madu & Madu indicated that, the main dissatisfaction of bank's customer's not using the ATM is the security and privacy, issues affecting ATM services (Madu & Madu, 2002).
Ihejiahi in 2009 expressed worries about the lack of cooperation among banks in the fight against ATM frauds now plaguing the banking industry. He stated that the muteness among banks on ATM frauds makes it difficult for banks to share vital information that will help curb the threat (Ihejiahi, 2009).

According to Obiano, the sudden rise of ATM frauds can be blamed on the careless issuing of ATM card by banks to customers, without considering the customer's literacy level. According to him, the major problems which lead to ATM fraud is when customers are careless with their cards and PIN numbers as well as their response to a phishing attack through e-mail and text messages asking them to provide their card details (Obiano, 2009).
In other research work by Diebold, he stated that, the major form of ATM fraud is PIN theft, which can be carried out in several forms; shoulder surfing, skimming, keypad recorder and camera, etc. This study clarifies that, the common type of ATM fraud perpetuated by criminals is PIN theft, which is mostly at over-crowding ATM points or terminals. The report further outlines other forms of frauds that respondents gave; card theft, force withdrawal and skimming at the ATM (Diebold, 2002)

(Cynthia, 2000) Stated that the 24 hours access to the ATM services in the banking industry has come to ease the burden of customer, but then, the ATM is a double edge sword, which has its own advantages and disadvantages with respect to security.

Chakrabarty (2013) stated that the banks' needs to improve the peripheral and system security in ATM locations and, at the same time, educate their customers about using their payment cards with due caution. He stated that whiles the bank does this, it will help protect customers from cases of fraudulent circulation of e-mails and SMS messages aiming at stealing customers bank details in order to defraud them (Chakrabarty, 2013).

ATMs crime has become a national issue that confronts not only clients of the banks, but also bankers and this financial criminal offence has risen rapidly in recent years (Onyesolu & Ezeani, 2012). Figure (6) gives the graph of ATM frauds from the year 2004 to 2010.

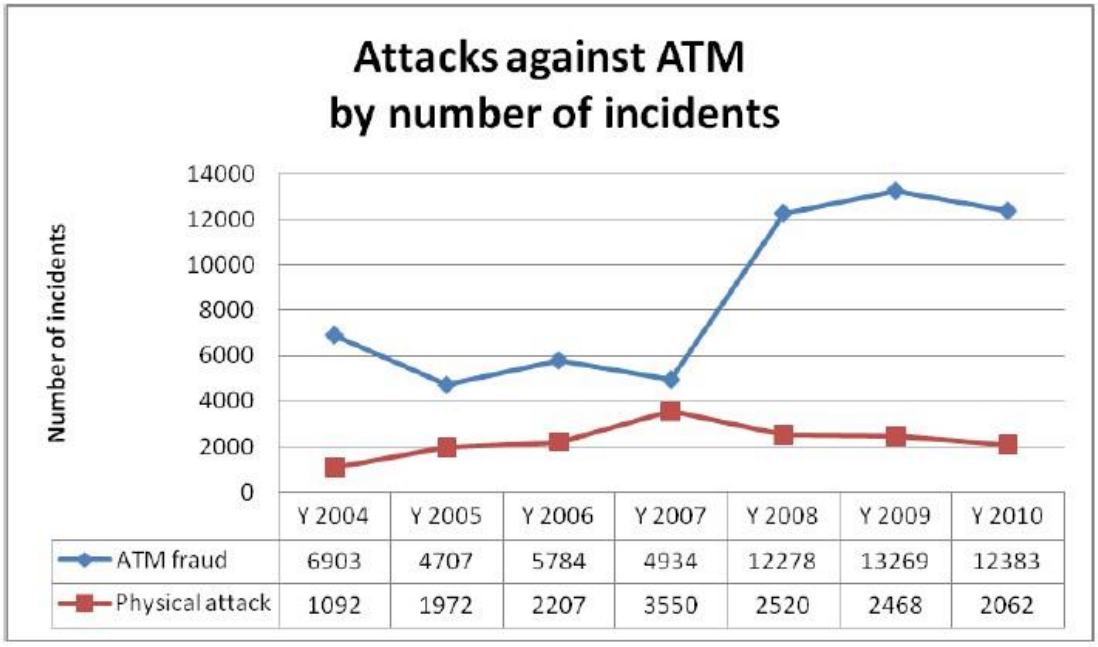

Figure 2.12 ATM related attacks. Source: (Onyesolu & Ezeani, 2012)

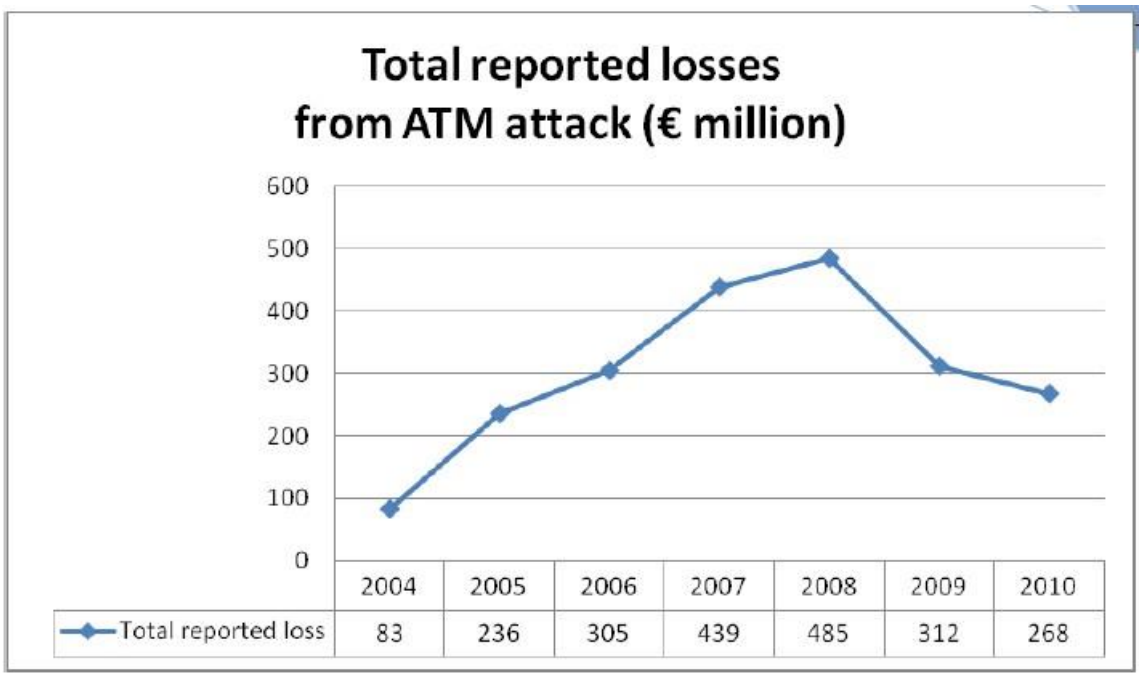

Figure 2.13 ATM Related attacks by total reported losses in Europe. Source: (Onyesolu & Ezeani, 2012)

Since the introduction of the ATM into the banking industry, a lot of concern has been raised by the general public and researches on its privacy and security, in agreement with (Madu & Madu, 2002), (Ihejiahi, 2009), (Obiano, 2009), (Cynthia, 2000), (Onyesolu & Ezeani, 2012), (Susmita, 2013) and (Chakrabarty, 2013) the security measures on ATMs should be enhanced to prevent most ATM frauds perpetuated by criminals and to boost the confidence of customers.

2.4.2 Research work on ATM security improvement

Some method and approaches have been proposed, from text, images and biometric to increase security on ATM. This section of the research looks at some of these techniques, from their strength to weakness.

An enhanced security for ATM machine with One-Time Password (OTP) and facial recognition features was proposed by Mohsin, et al., 2015 to enhance ATM security. The OTP was used for the enrichment of security of accounts and privacy of ATM users. The face recognition technology proposed in their system was to help the ATM to identify each and every user uniquely, by using faces as a key. The researchers concluded that, there are some little flaws associated with the face recognition technique, thus the failure to detect a face when aging, beard, caps and glasses. (Mohsin, et al., 2015).

ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System was proposed by (Sanjay, et al., 2014), the researchers acknowledged that, the PIN authentication system only, as used in most ATM machines is not secured. Hence, they sort to enhance the security system by introducing palm print recognition authentication as better and further mode of ensuring security at the ATM. The proposed method was accomplished with a prototype model of an ATM simulator that mimics a typical ATM system. In their conclusion, they recorded a percentage matching of 89.43% for palm-print recognition system and a rejection rate of 10.57% (Sanjay, et al., 2014). Thus, for 53 out of every 500 customers that will visit ATM's enhanced with this authentication system are likely to have problems with their transactions. Make a Force Rejection Rate of the system to be 10.57%.

Hirakawa in 2013 prospered a password enhanced mechanism called (Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks) to increase beefy up security on ATM, by preventing an observation attack for stealing user's password (thus video recording) and brute force attacks. Hirakawa acknowledges that the PIN authentication in traditional ATMs contributes to the immerse rising of ATM frauds, because this PIN, (password) are entered in open

spaces which gives a chance to criminals having a mobile phone equipped with cameras and miniature cameras to spy on the user whiles entering his/her PIN. To achieve this Hirakawa proposed two modules, basic method and an improved method. In their basic method, a correct entry position of each password must be provided beforehand. Whiles, in the improved method, a user does not need to provide any information beforehand, other than the password. In his approach, the alphabet board is randomize, thus the letters changes position all times, making it difficult for an observer to see the alphabet entered by the user (Hirakawa, 2013).

Lalzirtira proposed an authentication method called Graphical User Authentication to eliminate the defects in the alphanumeric authentication mode of traditional ATM's. In his research, he emphasized that graphical password which make use of images are easy for humans to remember than words or numerals. In his work he sounded that the introduction of the graphical password will eliminate the tendency of user written down their password, hence eliminating ATM frauds (Lalzirtira, 2013).

The use of images as a means of authentication in ATM system has its strength to some point and a big weakness to video recording, hence this method cannot be said to be a definite solution to ATM frauds.

A Dynamic Password (Dyna-pass) techniques was proposed to offer security to ATM transactions by Anand et.al, 2013. In their system, a user access the ATM with a debit card and his or her PIN as in the traditional system, but an SMS that contain a secret code called Dyna-pass is sent to the user mobile phone from the bank server if the PIN giving by the user is correct. The user then enters this new code received on his or her phone for confirmation, this again is checked with the

bank server for confirmation, and if correct ATM transaction access is given to the user (Anand, et al., 2013) . This implies that to access a user account at the ATM, you need his or his PIN, debit card and mobile phone. Hence a person close to the user can attain all these and defraud the ATM user. In this same paper an emergency third party authentication was proposed, whereby three to four people can register in the system with own mobile numbers for a friend. So that in the event that the actual account holder can't perform a transaction, these registered people can do transaction for the actual user through the mobile phone (Anand, et al., 2013).

Thus, in my understanding a user is given the chance to give three or four auxiliary phone numbers in addition to his or her mobile number.

Lawan proposed that, the fraudulent act associated with ATM's can be eliminated by the use of biometric authentication mechanism incorporated in the ATM security. In his report he looked at an overview of all ATM fraudulent activities and recommended approaches to element or prevents these frauds in ATM. In addition a prototype model for biometric authentication was developed to provide a solution to well-known security breaches in ATM authentication (Mohammed, 2011).

In other research work, a proposed neural network-based was adapted to match the fingerprint of users through the view of the blueprints and groove patterns of the fingerprints. This proposed module function perfectly on binary images and greyed scans; one good side of this proposed module is that, once a group is tracked, pattern can then be tracked with high accuracy. But this approach comes with a great threat where the network becomes inaccessible (Saropourian, 2009).

Multi-layers of convex polygon were proposed to implement fingerprint verification to enhance security levels on ATM's. In this work, extraction of fingerprint image was found in a specified area in which the prevailing brightness value of fingerprint ranges. The major limitation is the possibility of falsifying identity and falsified authentication cannot be noticed easily. To conclude these reviewed research efforts was carried out using a single biometric check without any form of cryptography, hence, could not warrantee a dependable security solution (Myo, 2009).

An authentication method called fakepointer is proposed to enhance the security levels at ATM's, which make use of a numeric key entry. With this approach, a disposable "answer selection data" is to be retrieved before each authentication. This selective information provides the background mark, like square, triangle, pentagon, hexagon of the numeric password displayed. At the authentication stage or period a user trikes the enter button, which adapts to the password according to the mark at the background.

This method is open to twice video recording attack, if the “answer selection data” can be safely retrieved before each authentication. However, this research did not emphasis on how to recover it safely (Takada, 2007) cited by (Takada, 2008).

Zhao & Li proposed an interface for PIN authentication called S3PAS, this mechanism proposed numerous characters to be displayed on an interface. A user at an ATM premises assigns three places where a password character is included in a triangle. This approach guides the user from shoulder surfing attack, but again if the input is recorded; it’s exposed to user password to criminal attacks (Zhao & Li, 2007).

A pin-Entry password authentication technique using numeric key entry was proposed. In this approach a black or white background is randomly displayed. The ATM user does designate a password rather he/she selects a black or white as background colour for a password. A user designates the background colour by the different colour pattern with four times to enter a password entry of One (1) digit. The method is very safe against shoulder surfing, but an attacker is able to video record the input operation the password is still open to attack. (Roth, et al., 2004) (Sakurai, et al., 2004;Sakurai & Munaka, 2008) proposed a text-password entry interface known as mobile authentication. With their method every text that is selectable are arranged in a square, with each text having its own background colour. For instance, every password is numeric or alphabetic, and the texts are ordered in 6×6 square in which six colours are used, with each colour appearing only once in each row. The colour pattern of a row is the permitted colour pattern of another row. In this approach, a user provides the correct background colour and a password beforehand. At the authentication (password entry) stage, the user changes the background colour of a pass-character until it matches the correct background colour, and then presses the accept/enter button. This technique comes with a restriction that all available texts must be displayed in the square, but this approach is secure against video attack by twice recording. Their techniques is applicable to numerical passwords but still, a 12-length numerical password is required for secure use, which might be considered too long by most ATM customers (Sakurai, et al., 2004;Sakurai & Munaka, 2008) cited by (Hirakawa, et al., 2013).

In this method, all of the texts available are presented as squares on the authentication interface. In the case of a four-character password, the columns number should be bigger than or equal to 10 for tolerance to random attacks, and the rows number should be larger than or equal to 9 for tolerance to video-recording attacks. Therefore, the numbers of available pass-texts are equal to or more than 90 for tolerance for both the attacks. And also, in a case where five-character password

is used, the columns number should be equal to or greater than 7 and the rows number should be equal to or bigger than 6. Therefore, the method is not used when four or five lengthy alphanumeric password is used as a PIN for authentication (Hirakawa, 2013).

A method called AWASE-E was proposed, which has 25 images, with one being a correct pass images. These images are normally displayed on the screen, similar to (Dhamija & Perrig, 2000) and (Passfaces, 2005) approach, but with the ability to display on a screen in where there is no pass-image. Where the pass image is not part of the images' on the screen, then a user has to select the "no pass-image button". Although this technique offers a quieter security to ATM authentication, it's only safe when taking a shot, is not clear to the attacker (Koike & Takada, 2003) cited (Hirakawa, 2013).

Passfaces Corporation proposed that an automatically created image is hard for a user to memorize, hence proposes the use of facial images as pass-images (realuser).
This method offers graphical passwords that utilize faces as a distinctive confirmation technology for safe logon. Users are given an arbitrary set of faces, usually three to seven which serve as a secret code for authentication in advance. An orientation is given to the users through a "familiarization process" that draws the faces in their minds. On the authenticate stage, a user has to pick out his/her designated faces, one at a time, from consecutive groups of nine faces (Passfaces, 2005) cited by (Hirakawa, 2013).

As far back as 2000, ATM frauds were a problem for banks, a method called Déjà vu was proposed to help reduce ATM frauds. In this method, a user, in advance selects five passes-images from

thousands of images produced by a computer. During the authentication stage, the user selects a pass-image from 25 images displayed on the screen and this image must be part of the previous five selected in advance (Dhamija & Perrig, 2000) cited by (Hirakawa, 2013).

The techniques proposed by (Dhamija & Perrig, 2000) and (Passfaces, 2005) are exposed to shoulder surfing attack, because the user designates a pass-image in the process of authentication.

In 2010 the UK identity card scheme was analysed by (Shaikh & Rabaiotti, 2010). Their analysis viewed the scheme from the standpoint of high size public deployment, and described a trade-off triangle model. In their research Shaikh & Rabaiotti established that there exists a trade-off among several characteristics, i.e., Privacy, precision and scalability of a biometric based identity management system, where stress on one weakens the other.

(Ratha, et al., 2001) Proposed an embedded fingerprint system for ATM security applications, in their proposed system, bankers will have to collect customers' finger prints and mobile numbers while opening new accounts. With their system a customer wanting to perform a transaction at an ATM will get a text of a 4-digit code message on his/her GSM phone when the customer place a finger on the finger print module attached to the ATM. This message is automatically generated every the customer visit the ATM. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access. The main disadvantage of this system is that customers with a lost phone needs a new one or has to updates his records at the bank before he/she can access his account on an ATM.

An ATM enhancement technique using secured Personal Identification Image (PII) process was proposed by Santhi and Kumar. This method is secured against shoulder surfing attack, but if a recording camera is hidden to record the authentication process, the system becomes insecure (Santhi & Kumar, 2012).

A highly authenticated biometric security system is proposed by (Subh & Vanithaasri , 2012), to enhanced ATM security. The proposed method implementation however lacks the strength to exclude wrong or false feature and minutiae points from its extracted list.

2.5 Why fingerprint

Considering the review above, it is clearly shown that, the best authentication system for the ATM is to employ a biometric techniques, authentication system, but here lies the question, which biometric technique is appropriate?

A survey conducted by the International Biometric Group (IBG) in 2004 on comparison between the uses of biometrics features, employed for system security, shows that fingerprint has a market share of 48% compared to all other biometric features (Iwasokun, et al., 2012)

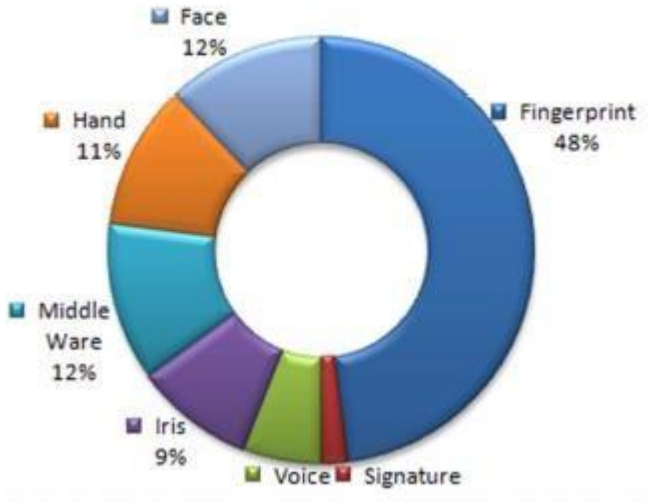

Figure 2.14 Comparative survey of fingerprint with other biometric features in 2004. Source: (Iwasokun, et al., 2012)

From the result it can be deduced that there is significant increase margin between the uses of fingerprint for identification to other biometrics such as hand, face, middleware, signature, voice, and iris (Onyesolu & Ezeani, 2012) cited by (Iwasokun, et al., 2012).

The following were the reasons attributed to the huge margin of existence (Iwasokun, et al., 2012).

1) There is a wide variation in fingerprint, thus fingerprint differ from person to person.
2) The existence of high degree of dependability and consistency in fingerprint, thus the fingerprint of a person can or may change with respect to scale but not in relative apperance. Which is not the same in other biometrics.
3) Fingerprint traist are left each there is a contact with the finger.

Again the larger use of personal identification employing fingerprint was attribute to the following reasons.

1) Easiness and affordability of gotten fingerprint capture devices
2) The existence of high speed computing hardware.
3) The express growth of Internet and network transactions.

4) The growing awareness of ease-of-use module for dependable security.

According to Jain et al. cited by (Klokova, 2011), the high dependability and user approval of fingerprint biometrics' are justified by reasonably low scanning devices cost, user friendly and high authentication process accuracy and speed.

2.6 Conclusion

In light of the above discussions, it appears clearly, that the PIN and Image's authentication approach does not guarantee sufficient ATM security. A good authentication technique is expected to be tolerant to video-recording attacks (Hirakawa, et al., 2013). In an authentication process, replacing the combination of possession (cards) and knowledge (pins) with only biometrics for more convenience does not automatically lead in a higher security level. Biometric technology is one the secured and best way of eliminating these problems associated with ATM security threats (Anil , et al., 2010).

A person, biometric data is a strong bond between the person and his individuality, this is true because biometric identities cannot be easily split up, duplicated or lost. Hence, biometric identification is basically superior and more immune to social engineering attacks than the two (passwords and tokens) traditional methods of identification (Mudholkar , et al., 2012).

Biometric or three factor authentication system is considered as the strongest and the best authentication techniques systems. It is extreme better and secure than traditional authentication systems such as knowledge and token authentication based system, thus behavioural or psychological characteristics/traits of a person or human is permanent, nontransferable and cannot be stolen. Hence biometrics can be said to be the only form of authentication system that requires the physical presence of the system user (Khan, 2010).

The finest application of biometric authentication in the financial industry still requires at least one more authentication method that e.g. combines with knowledge and/or possession features or that demands two biometric features (Graevenitz , 2007) cited by (Hirakawa, 2013). To solve or minimized the current growth of ATM frauds problem biometric authentication technology and sneak-shot camera-detection technology must be implemented on the ATM (Hirakawa, 2013). Hence, research is needed to beef up ATM security. This thesis therefore proposes a multifactor authentication of a Fingerprint and a PIN mechanism to improve security levels at the ATM system.

To achieve this, this work sort to improve on the fingerprint authentication presented by (Subh & Vanithaasri , 2012), by eliminating false minutiae from its fingerprint database. And also enhancing the work presented by (Santhi & Kumar, 2012; Iwasokun & Akinyokun, 2013), by designing an application instead of simulations.

Chapter 3

METHODOLOGY

3.0 Introduction

This chapter of the thesis outline the materials, methods and approaches used in modelling and designing of the multifactor (PIN and Fingerprint) ATM authentication system.

3.1 Materials Used

This section presents the details of tools and materials required for the implementation of the proposed ATM multifactor authentication system.

3.1.1 Fingerprint Image Scanner

A fingerprint serves as a key or password to the proposed multifactor ATM authentication. Thus, a fingerprint image serves as material input to the ATM system. To acquire this information, a fingerprint scanner is required. Figure 3.1 depicts a snapshot of the fingerprint scanner used in this thesis. It is an electronic scanner that scans the thumbprint of a user and save it as an image. The image to be save goes through the proposed image extraction, enhancement, normalization and binarization methods. The scanned fingerprint is finally stored in a database as a template during user enrollment and compare (authenticates) it with the user's thumbprint during an ATM transaction

Figure 3.1 A Fingerprint Scanner

3.1.2 Software Development tool

Microsoft Visual Studio 2010 (C#) was used to develop the front end, where system user can graphically interact with the ATM.

The back end (database) was developed with Microsoft Structured Query Language (MSSQL) server 2008, MSSQL is a relational database management system (RDBMS) use for creating a database for Microsoft Windows family of servers. MSSQL was chosen over other database management tool, due to its ability to provide a working environment to easily generate a database that can be easily and quickly accessed from the internet, workstation, LAN and so on. The server also uses a relational database management system that gives different type of administrative tools, which help to ease the burdens of database development, maintenance and administrations.

To help communicate between the fingerprint scanner a Grfinger software development kit (SDK) was employed in conjunction with the Microsoft visual studio to help in the implementation of the proposed fingerprint enrollment and authentication algorithm.

3.2 Methods Used

3.2.1 Design Criteria and Concept

Fingerprint as a means of a person's identification, was introduced a long time ago and it is accepted, that the fingerprint of every person is unique. Hence fingerprint matching is universally considered as one of the most dependable techniques of identifying a person.

Figure 3.2 portrays the block diagram of the proposed ATM multifactor authentication system, which comprises of customer account details, PIN database, fingerprint database and an ATM machine. In the software development process, the standard Software Development Life Cycle (SDLC) model and Object Oriented Analysis and Design (OOAD) model are used in the design and implemented stages.

The following subsections explain in details how the proposed ATM multifactor Authentication will enhance the level of security on the ATM, to safeguard the users of ATM from various ATM attacks initiated by fraudsters.

The internet, is the first phase of the proposed system, serving as the working environment and platform for the proposed system to communicate between individual ATM terminals and the central bank server. Customers fingerprint and PIN databases are available on the bank servers and a relational database model is used for storing information on the fingerprint and PINs of all registered customers. These information include pattern type, and feature characteristics.

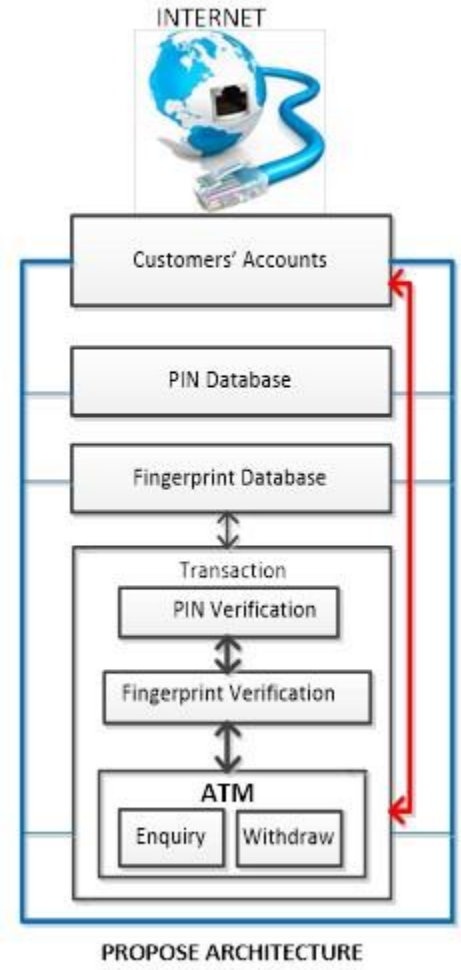

Figure 3.2 Conceptual Design of Proposed ATM Security Structure.

Figure 3.3 shows the flowchart for the PIN and fingerprint verification components proposed for verifying the authenticity of a user. A user who is already enrolled onto the proposed system, will have to go through the verification process presented in figure 3.3.

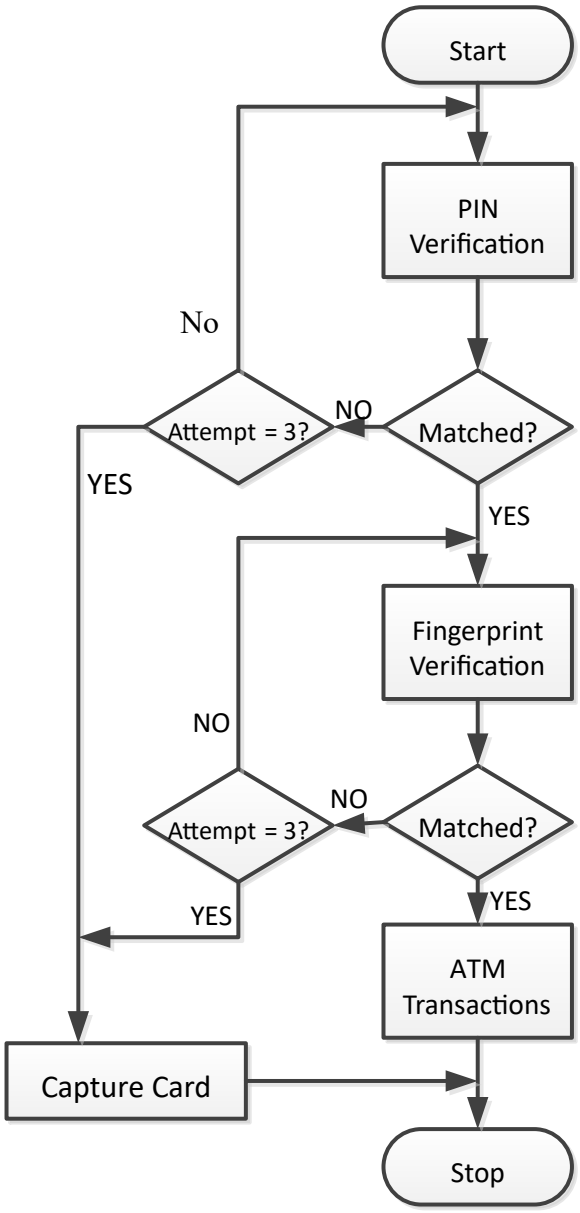

Figure 3.3 Flow Chart of Proposed System

User Fingerprint enrolment involves enhancement, feature extraction and matching and storage as shown in Figure 3.4.

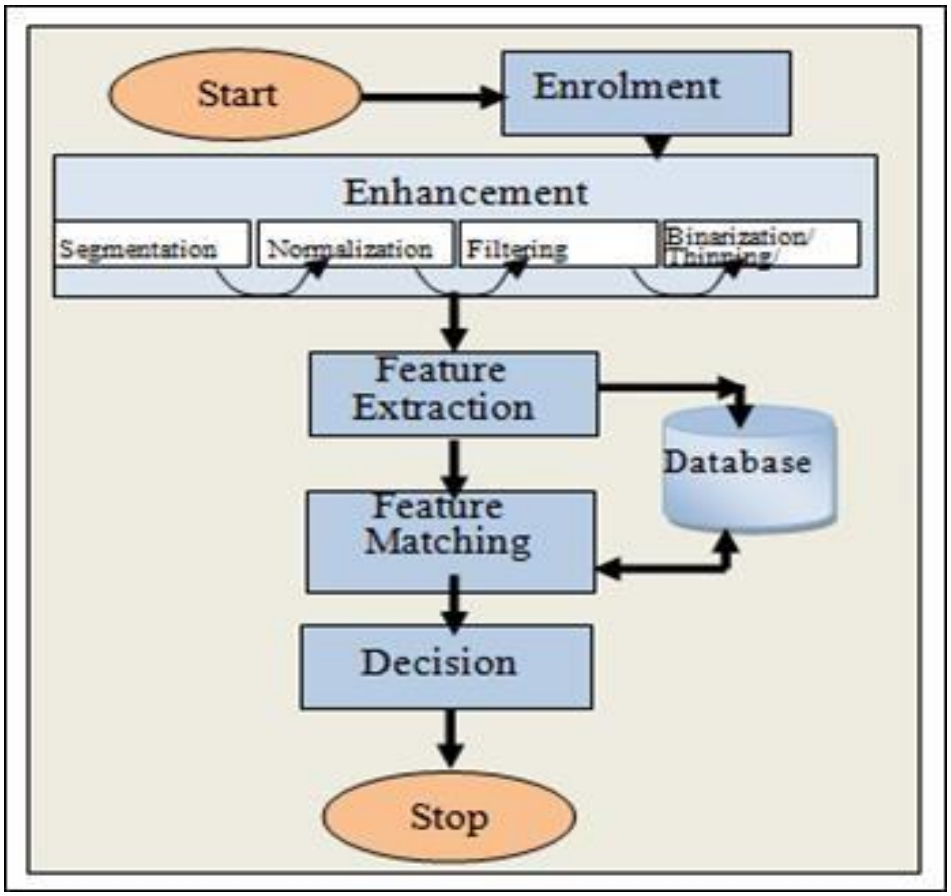

Figure 3.4 Block Diagram of User Fingerprint enrollment

For the period of image enhancement, the foreground regions of the image which are the regions containing the ridges and valleys are separated, from the background regions, which consist mostly of noise. Segmentation is performed with the view of ensuring that focus is only on the foreground regions, while the background regions are ignored. The segmented fingerprint image ridge structure will be normalized so as to standardize the level of variations in the image grey-level values. By normalizing, the grey-level values will be brought to a range that is good enough for improved image contrast and brightness. The normalized image is then filtered to remove any noise and spurious feature present. The filtering will also preserve the true ridge and valley, and this involves the ridge orientation and frequency estimations. The output obtained after filtering

(filtered image) is converted to binary format and thinned for satisfactory feature extraction. At the feature extraction stage, major features; namely ridge ending and bifurcation are located and extracted from the image. These two main features are the characteristics that establish uniqueness among different fingerprints.

The extracted features from the user template is matched with templates of the other images in the database. A user of the ATM will provide his or her PIN and if it's correct after system check, then the user is granted access to the second level of authentication (fingerprint identification), when the fingerprint of the user is scanned by the fingerprint model incorporated in this system and a match exit when compared to the one in the database during the enrollment of the user, access is granted to the user to perform his/her ATM transactions.

The performance evaluation criteria of this design are as follows:

- False Match Rate (FMR) or False Acceptance Rate (FAR)
- False No match Rate (FNMR) False Rejection Rate (FRR)
- Failure-to-Enroll Rate (FTE) System Failure-to-Enroll Rate
- Total Error Rate (TER)
- Efficiency
- Complexity of Implementation

False Match Rate (FMR): this is when the system matches a user's fingerprint template extracted for verification with a different user's enrolment template in the database. Thus, this can be explained as an imposter being recognized by the system as a rightful user. This is generally the most critical accuracy metric, as it's a good system security design to keep imposters out in most applications.

False Non-match Rate (FNMR): this Error appears when there is a mismatch of a legitimate user's verification template with his enrollment template. This can be explained as a rightful user not being recognized by the system. Even though FNMR is not serious as FMR, high false, matching in a system can lead to low productivity and frustration of users.

Failure-to-Enroll Rate (FTE): this type of error happens when the system fails to take out consistent, unique and replicable characteristic from the sample presented whiles enrollment. Thus the system is not able to create a new enrollment template for a new system user. This error can be attributed to user behavioural reasons, such as the movement of an enrollee during the data acquisition process and physical reasons, e.g. wear and aging of the enrollee causing faint patterns.

3.2.2 Fingerprint Identification Algorithm

The good nature of a fingerprint image in terms of the adequacy level of the implementation algorithm as well as quality are part of the basic deterministic parameters of the performance level of Automatic Fingerprint Identification Systems (AFIS) in their various assigned tasks (Iwasokun, et al., 2012).

This thesis employs a Fingerprint Identification System presented by Shallita, et al., (2010). The algorithm by Shallita, et al., (2010) involves two main processes namely enrollment and authentication.

The enrollment process is where a person’s fingerprint is captures using a fingerprint capturing device and saved in a database.

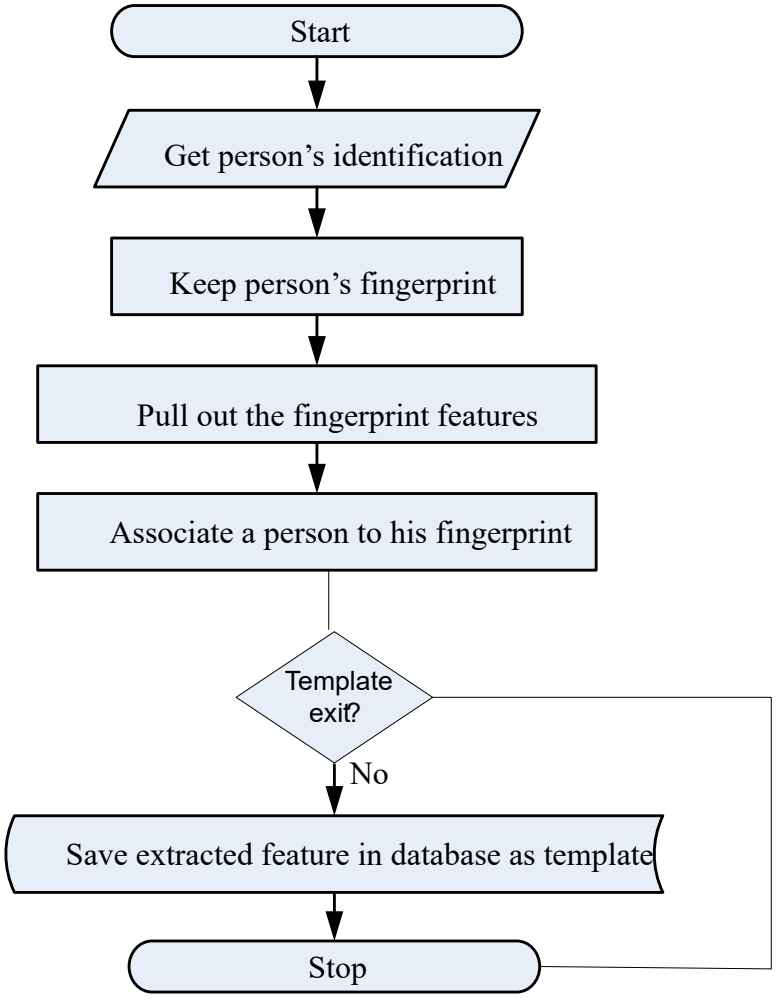

Figure 3.5 A flow chart for fingerprint enrollment process

Figure 3.5 shows the flow chart for the enrollment phase. The fingerprint of a user is captured with a fingerprint scanner, feature is extracted as a template and then save in the database.

The authentication is a process where a person claiming to be whom he or she is, is verified. This process consists of a comparison between a captured fingerprint at the ATM terminal to an enrolled fingerprint template stored in the database, in order to determine whether there's a match, and if there is a match, the user is permitted to conduct his or her ATM transactions. This process is as shown in figure 3.6.

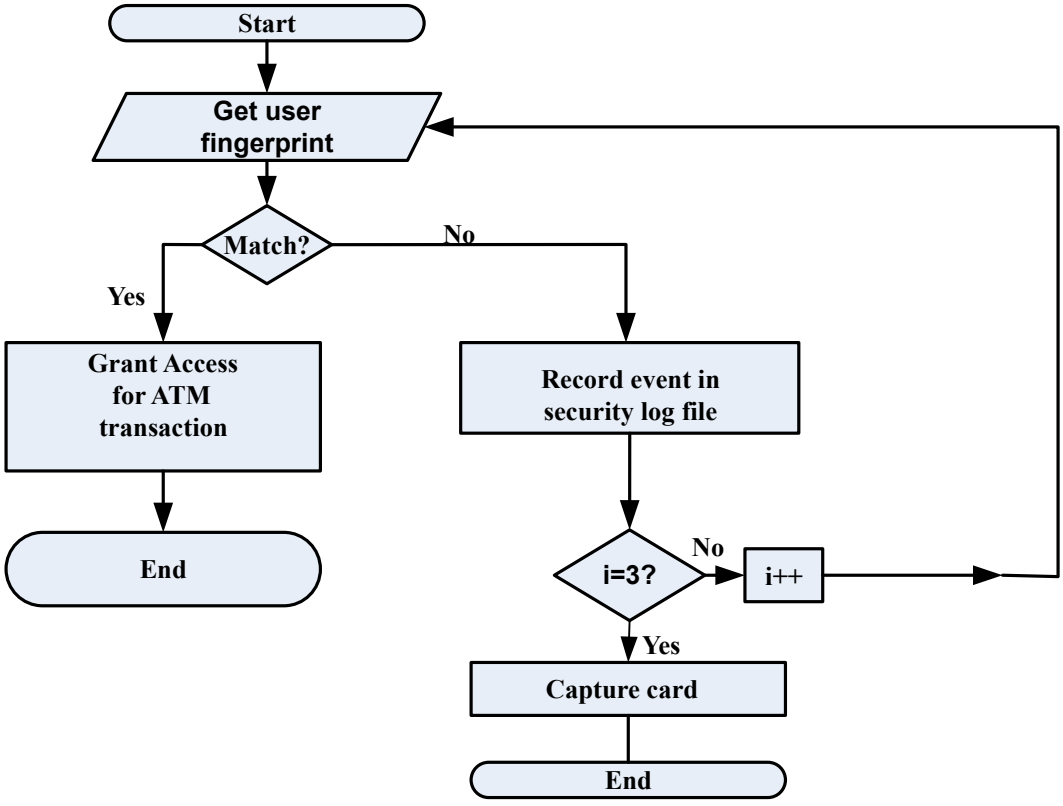

Figure 3.6 Authentication Process Flow Chart

3.2.3 Steps for Fingerprint Image Processing

The following section describes in details the various steps and methods employed for the extraction, enhancement and binarization of the fingerprint image scanned with the image scanner.

3.2.3.1 Fingerprint Image Enhancement

The dependability and authenticity of fingerprint technology employed in an AFIS are preceded with proper detection and extraction of features in the fingerprint image. To obtain proper and

sound feature extraction from any fingerprint, such fingerprint must be enhanced first. A well enhanced image brings about clarity in separation between spurious minutiae and valid ones. Minutiae points created as a result of artefacts or noise are called spurious minutiae. This research work adapts the algorithm proposed by Babatunde, et al., 2012 and Iwasokun, et al., 2012 for image enhancement with little modification. The main steps of this approach are image/ridge segmentation, ridge/image local normalization, ridge filtering and ridge binarization/thinning.

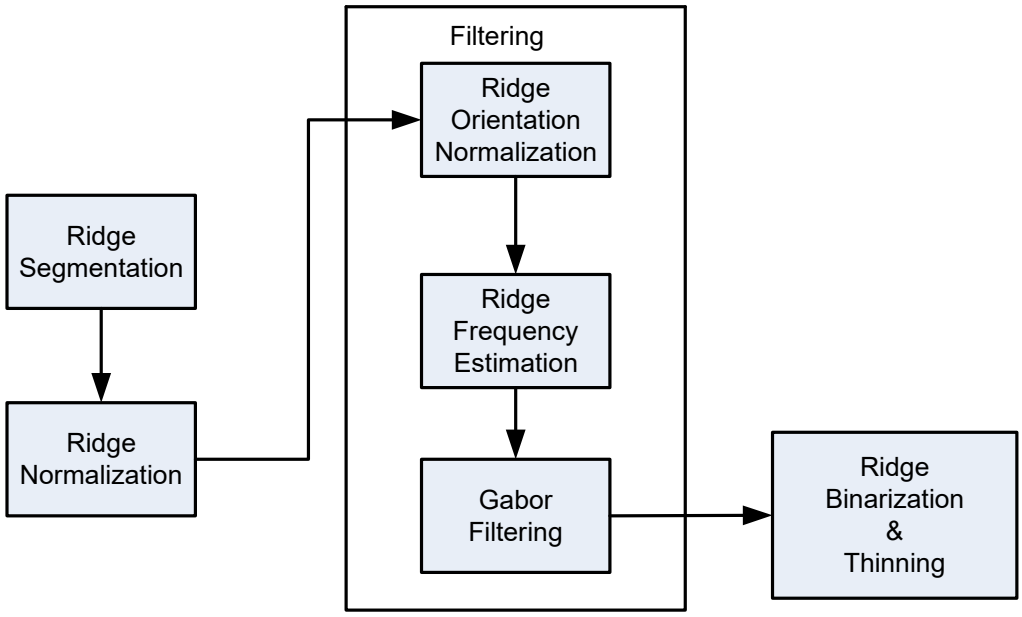

Figure 3.7 The Conceptual Diagram of the Fingerprint Enhancement Algorithm

3.2.3.2 Image Segmentation

All fingerprint images are described by two regions, namely foreground regions and background regions. The valleys and ridges are in the Regions of Interest (RoI) or foreground regions as shown

in Figure 3.8. These regions are called the RoI, because they contain the feature points. During enrollment, some noise is introduced into the image, this happens outside the foreground regions and are called the backgrounds as shown in Figure 3.9. The importance of the segmentation is to separate the foreground regions from the background regions of the image, this paves way for a reduction in difficulty accompanying preceding stages of the image enhancement by making sure that the focus is only in the foreground.

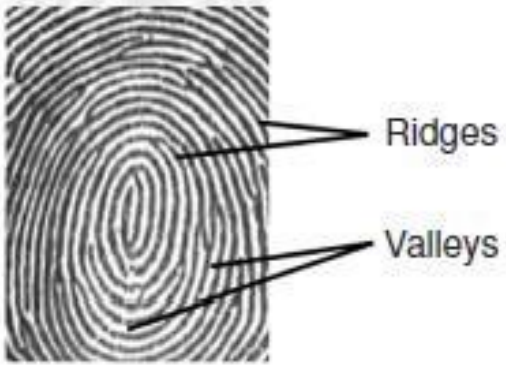

Figure 3.8 Ridges and Valleys on a Fingerprint Image

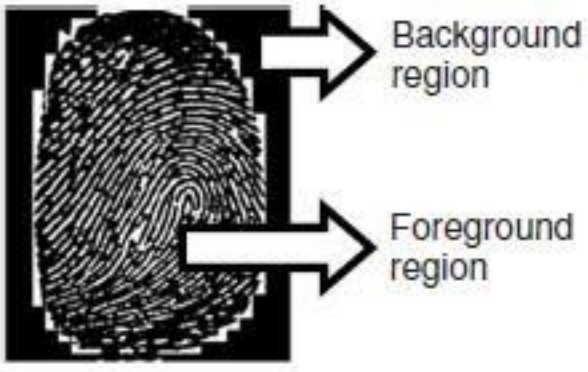

Figure 3.9 A Fingerprint Image and its Foreground

The foreground region holds very high grey-level variance values, whiles the background regions holds very low grey-level variance values.

The grey-level variance values are obtained through a block processing approach instead of pixel approach (Thai, 2003) cited by (Iwasokun, et al., 2012) and (Babatunde, et al., 2012). With block processing methodology, the first stage is to divide the image into a square block size (W x W) whiles obtaining the variance, $V_{(k)}$ for every pixel in k^{th} with equation 3.1 and 3.2.

$$V^{(k)} = \frac{1}{W}\sum_{i=1}^{W}\sum_{j=1}^{W}(I(i,j) - M(k))^2_2 \tag{3.1}$$

$$M(k) = \frac{1}{W_2}\sum_{c=1}^{W}\sum_{d=1}^{W} J(c,d) \tag{3.2}$$

From equations 3.1 and 3.2 $I\ (i,j)$ and $J\ (c,d)$ are the grey-level values for pixel (i,j) and (c,d) respectively in block k.

3.2.3.3 Image Normalization

The output of the image ridge structure obtained after segmentation is normalized to standardize the grey-level values that make up the image. By normalizing the image, the grey-level values are restricted to an acceptable range that is good for improving brightness and contrast. The first process in the normalization proposed (Iwasokun, et al., 2012) is embraced in the research work, thus dividing the segmented image into various blocks of size S x S. A comparison is then made with each grey-level pixel in the segmented image and the average grey-level value within the host

block. Assuming for comparison, M_o and V_o are used as mean and variance, respectively, then for a pixel $I(i, j)$ which belongs to a block having M as average grey-level, it comparing result produces an output normalized grey-level value N(i,j) which is computed from the equation.

$$N(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{V_0(I(i,j) - M)^2}{V}} & if\ I(i,j) > M \\ M_0 - \sqrt{\dfrac{V_0(I(i,j) - M)^2}{V}} & otherwise \end{cases} \quad 3.3$$

3.2.3.4 Image Filtering

Spurious and noise features are removed from the normalized image whiles valley and ridge structures are preserved by filtering the normalized fingerprint image. The following fingerprint image structure is employed in this research work:

Orientation Estimation

In a fingerprint image filtering orientation estimation is a prerequisite. For all fingerprint images, flow patterns of different directions are formed by the ridges. The arrows in Figure 4.6 shows a flow direction of the ridges at nodes A and B over a range of pixels, and ridge orientation is indicated by α and β respectively.

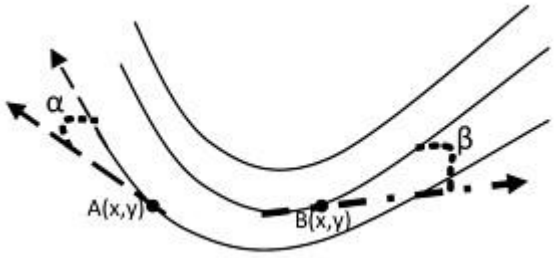

Figure 3.10 The Orientation of a Ridge Pixel on a Fingerprint.

The algorithm proposed by this research for fingerprint ridge orientation is a modified version of the Least Square Mean (LSM) algorithm proposed by Babatunde, et al., (2012); Iwasokun, et al., (2012) and Thai, (2003).

1. First and foremost, blocks of size S×S were formed on the normalized fingerprint image.
2. For each pixel, (p, q) in each block, the gradient magnitudes in the x and y directions being represented by gradients ∂_x (p, q) and ∂_y (p, q) are computed, respectively. Thus, employing horizontal Sobel operator for ∂_x (p, q) and vertical Sobel operator for ∂_y (p, q)

$$\begin{matrix} 1 & 0 & -1 \\ 2 & 0 & -2] \\ 1 & 0 & -1 \end{matrix} \qquad \begin{matrix} 1 & 2 & 1 \\ [0 & 0 & 0 \\ -1 & -2 & -1 \end{matrix} \qquad (3.4)$$

Horizontal Sobel Operator Vertical Sobel Operator

3. The S x S neighborhood in (Thai, 2003) and (Iwasokun, et al., 2012) is used to calculate the local orientation of each pixel within the fingerprint image. But this research sort to do a little modification in this research, thus the image is divided into S x S block while the local orientation for each block centered at pixel I (i, j) was calculated. With $\theta(i, j)$ being the LSM estimate of the local orientation at the block centered at pixel (i, j)
4. The oriented image is put into a vector of continuous field
5. Apply Gaussian smoothing on the vector field.

Ridge Frequency Estimation

Ridge frequency estimation is the next prerequisite for fingerprint image filtering. In all fingerprint images, there exists a local frequency of the ridges, which jointly formulate the ridge frequency image. This ridge frequency is obtained by extracting the ridge map from the image (Iwasokun, et al., 2012).

Gabor Filtering

A finger structure is obtained from the fingerprint image with Gabor filtering after obtaining the prerequisites. The Gabor filtering process involves the removal of artefacts and noise, by employing the formulae (Iwasokun, et al., 2012):

3.2.3.4 Image Binarization and Thinning

The output filtered image from Gabor filtering in converted into binary for better performance. The image binarization technique, proposed by (Iwasokun, et al., 2012) is used in this research with a threshold assumption (T) that reduces overlap and enable a good separation within clusters. The steps outline to determine the true value of T, is as follows:

1. Separate the pixel into two clusters with respect to the threshold
2. Determined the then of each cluster
3. Square the difference between the mean
4. Determine the product of the number of pixels in each cluster

The difference between the clusters means determines the operational success of the process. The threshold (T) is said to be at optimal when it maximizes the variance of between-class or,

contrariwise, the value that minimizes the within-class variance. For each cluster its within-class variance is calculated as the absolute sum of the variance. Details of the fingerprint image enhancement, extraction and binarization algorithm can be found in (Iwasokun, et al., 2012)

3.2.3.5 Fingerprint matching and decision-making module

The matching process is one of the difficult stages in the fingerprint authentication system, due to quality in deviations of the fingerprint from the same user, as time changes. These variations are due to changing noise due to sensor malfunction, skin conditions, changes in ambient conditions and errors produced during extraction. At this level the extracted features from the clients during enrollment are compared with the stored templates in the database. With fingerprint-based biometric environment, a matched score is determined from the number of match minutiae existing between the input and the stored template feature sets. The match score is dependent on the quality of the biometric data presented. The matching module has a decision module, which uses the match score to authenticate a claimed identity or gives a ranking of the enrolled individualities in order to identify an individual. Some of the fingerprint matching techniques are

1. Minutiae-based matching,
2. Correlation-based matching,
3. Ridge feature-based matching.

Minutiae-based matching

The minutiae based matching hinge on the orientation and position of minutiae points acquired from a fingerprint. In this work, minutiae established fingerprint recognition is performed by using

the algorithm developed. This algorithm generates a score based on pairing minutiae of the fingerprints.

Correlation-based matching

Two fingerprint images are overlaid and the relationship (at the intensity level) between matching pixels is calculated for different orientations. This matching approach is becoming more popular fingerprint authentication process. This approach gives High matching accuracy. In correlation method matching of fingerprint is done from grey-level information is taken. The correlation based approach is one of the approaches employed when a good fingerprint image can't be obtained, in this situation's extracting minutiae might be difficult. Nevertheless, correlation based approach cannot be used in several applications due to its large computational effort (Sainath & Tangellapally , 2010).

Ridge feature-based matching

Ridge feature maps can also be used for fingerprint matching. The approach utilises both orientation and frequency data, and eliminates the requirement of minutiae detection in the fingerprint. Minutiae abstraction is difficult in low-quality fingerprint images, whereas other features of the fingerprint ridge pattern (frequency and local orientation, ridge shape) may be extracted more reliably than minutiae. The approaches belongs to the categories that relates fingerprints in terms of feature extraction from the ridge pattern (Sainath & Tangellapally, 2010).

3.2.4 System Design Approach

The Waterfall (linear-sequential life cycle) model design methodology was employed in the designing of the proposed algorithm, this model is the mother and father of all SDLC models, and it is simple to understand and use. With a waterfall model, the output of a sub-model becomes the input to another sub-model. By the use of this model approach to this research, it gave the ability to group the task to specific groups or sub module for managerial manipulation of each sub-model. Figure 3. 11 shows the pictorial representation of the various stages/phases associated with the waterfall model.

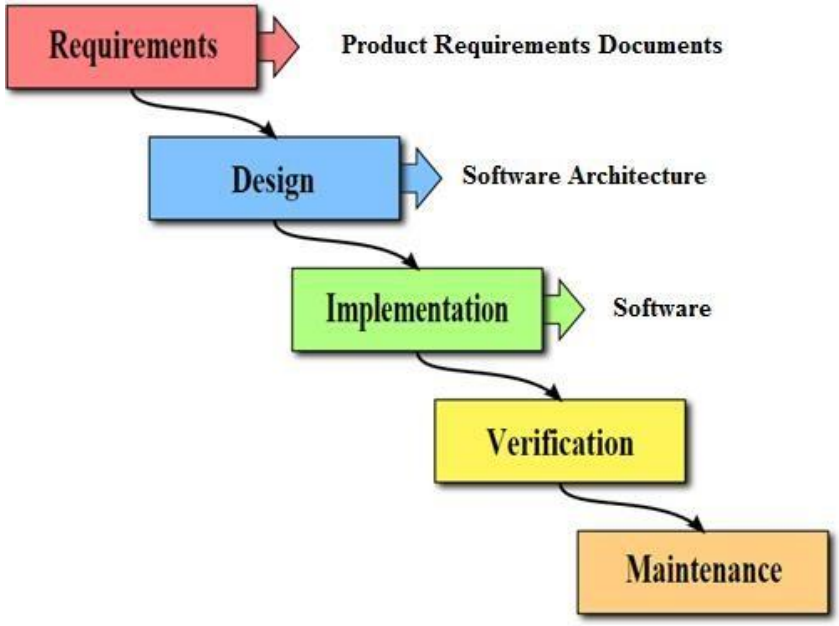

Figure 3.11 Waterfall model

The *Requirement Gathering*: This stage allows for the gathering of all the requirements of the system to be produced/developed, analysed and documented in a prerequisites specification document.

System Design: The requirement specs obtained from the first stage/phase are studied under this phase and system design is carried out. This phase helps to outlining the hardware and system specification and helps in overall system architecture defining.

The *Implementation*: At this phase of the application design, the output of the system design stage is developed in small units (programs), with each unit developed is tested for its quality of being suited to serve its defined purpose very well, this is also called Unit Testing.

Integration and deployment: Under this phase of the waterfall model all program units developed under the implementation stage are merged into one system after testing of separate units. The whole system is tested for any failures and errors. If no errors and failures are found, the system is deployed to the customer.

Maintenance: There might be some matters which rises up in the client environment, and to mend these problems patches are released. For product enhanced and sustainability, periodical version with better operational qualities are released. Maintenance is carried out to effect these changes within the customer surrounding.

3.2.5 Software Modules Design

As a requirement of the approach used for implementing the proposed algorithm, five primary phases were required for producing consolidative software levels necessary to meet system

objectives and goals. Each module design and tested separately, and then combine together to form a complete application.

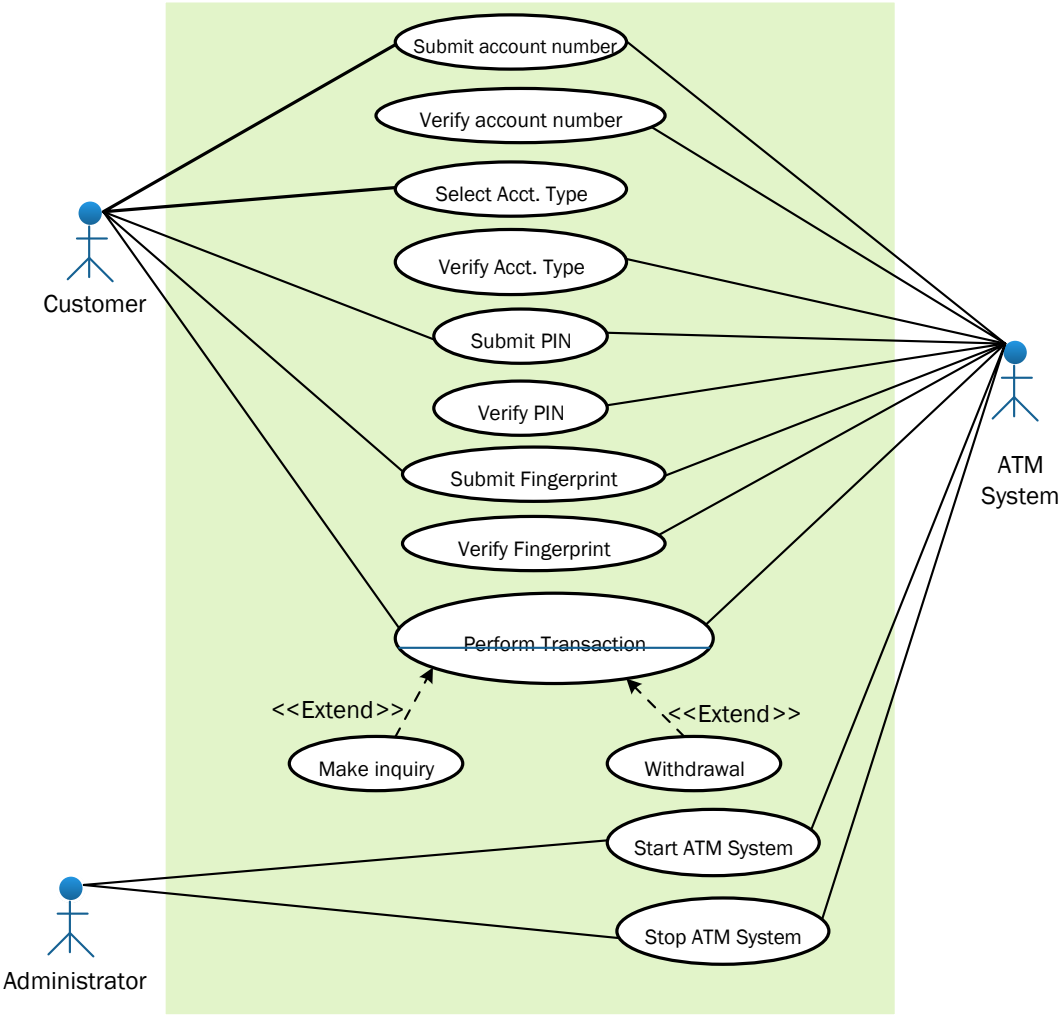

Figure 3.12 Use Case Diagram for Proposed ATM Multifactor Authentication Module

Figure 3.12 shows the Use Case Diagram for the proposed ATM multifactor authentication module. The primary actors; Administrator and customer and secondary actor; ATM system triggers the use-cases. Figure 3.13 shows the a pictorial view of the different functions, windows forms, user controls and the relationships that exist between various sections of the program codes, and how each program code interact with another section.

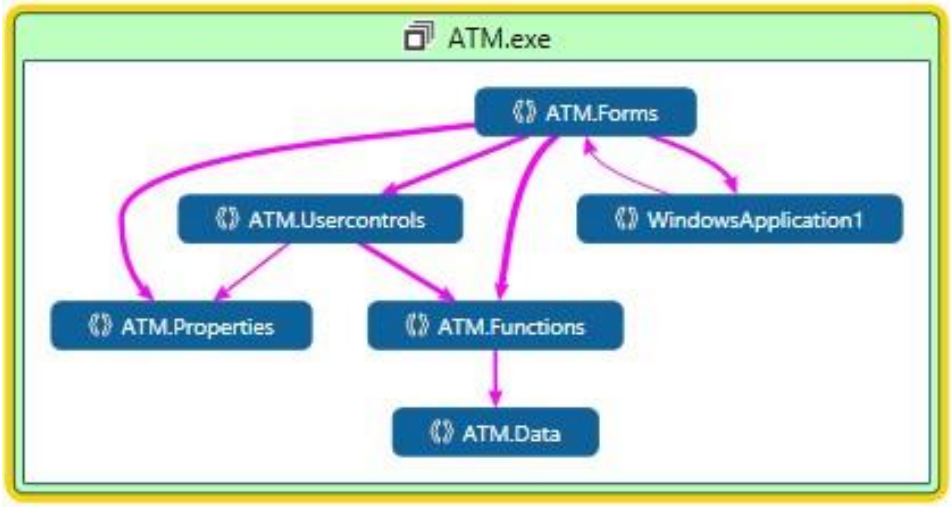

Figure 3.13 Code Map and Relations

Figure 3.14 gives a further details into sub modules and function the exist within the main modules

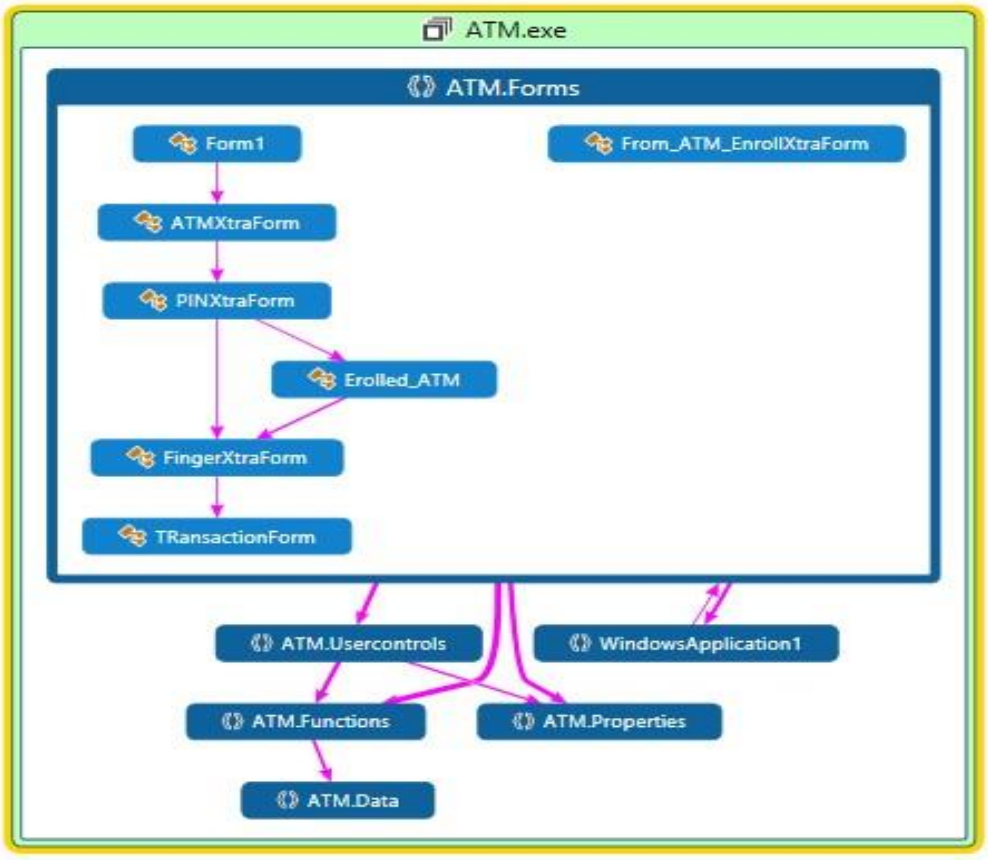

Figure 3.14 Detail Code Elements and Relation

3.2.5.1 Customer Enrollment Module

The first module is the user/customer enrollment module. This module helps in capturing the user/customer fingerprint and associate it with his/her PIN and account details in the bank central database.

The enrollment of user into the system is by two means:

1. A user can be enrolled onto the fingerprint database from the bank premise.
2. Alternatively a user can also register from the ATM terminal.

Bank Premises Enrollment Module

Figure 3.15 shows the enrollment from the bank module. This module enables the bank to enroll customers that come to the banking hall directly to be enrolled into the system.

Figure 3.15 Module for Customer Enrollment onto the Fingerprint System from bank hall ATM enrollment module

The enrollment from the ATM module differs a little from that of the banking hall enrollment module, in that for a customer to be enrolled from the ATM, he/she needs to confirm a secret code sent to him/her from the bank server onto his/her phone details she/he gave to the bank during his/her accounts opening processes. This module is displayed to the ATM users that are not enroll onto the fingerprint database, when they visit any ATM equipped with this proposed system after entering their PIN and checks are correct. Figure 3.16 shows the module.

Figure 3.16 Module for Customer Enrollment unto the Fingerprint System from ATM

3.5.2.3 Welcome Screen Module

This screen displays a welcome message to users/customers that come to the ATM for transactions.

It prints a welcome and an instructional message “Please Insert Your Card” on the screen of the ATM to the user. If the card is authenticated as a valid card, access is given to the user/customer to enter his or her PIN code for verification and access to enter the next step of the transaction.

Where a valid card is;

1. A card designed for ATM transactions, not every plastic card is accepted by the ATM.
2. The card is designed for the said ATM, since some ATM’s don’t accept visa the card must be checked.
3. The expiring date of the card is not due.

Figure 3.17 Welcome Screen for Customer at ATM centre

3.5.2.4 PIN Entering Module

This module is displayed to the ATM user if and only if the card inserted by the user is a valid one. The screen prompts the user to enter his or her four digit PIN, by display “Please Enter Your PIN” on the screen, The PIN is encrypted and sent to the database for a comparison with the PIN stored

in the database again the customer ID and account number. And if there is a match, access is given to the user to enter the last authentication level.

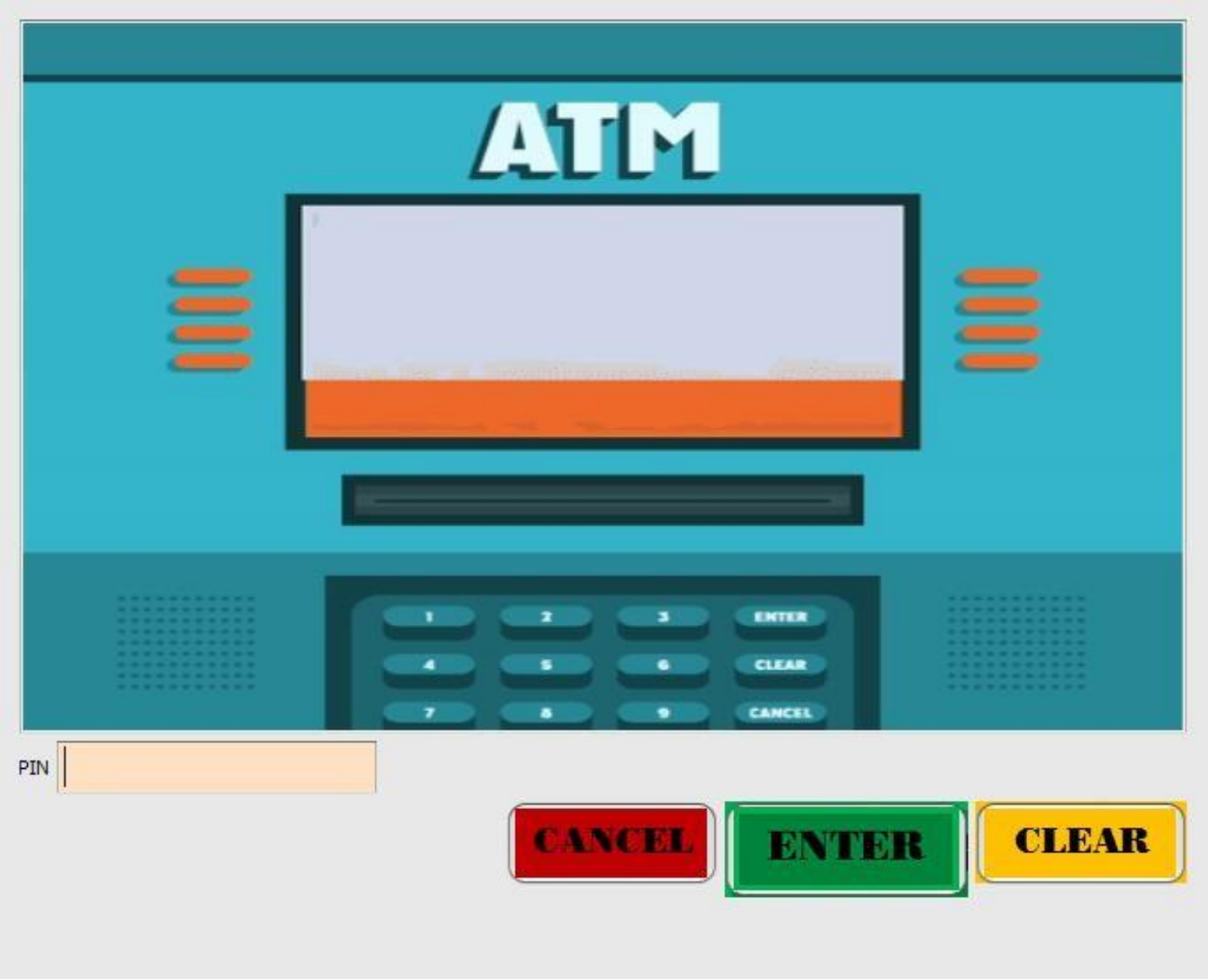

Figure 3.18 PIN Authentication Module

3.5.2.5 Fingerprint Authentication Module

The user is sent to this module when his her PIN authenticity is true. This is the last stage in the authentication level of the proposed multifactor authentication security level. This is the only stage that authenticates the holder of the card to verify if he or she is the true owner of the accounts he

she want to access. Because at this level fingerprint cannot be transferred to a different person. A message is displayed on the screen telling the user to put his or her thumb or the fingerprint scanner attach to the ATM. The scanner takes the fingerprint/thumbprint of the user as image, when it senses a finger/thumb on it and a comparison is done with the template stored in the database during user enrolment and if there is a match access is given to the user to perform his or her transactions.

A user is given three chances in all authentication stages, and if he/she fails in all these three chances at any of the authentication stages, his/her card is captured by the ATM.

Figure 3.19 Proposed Finger Print Verification Module Interface

RESULTS AND DISCUSSIONS

4.0 Introduction

This chapter present implementation results and their discussions for the PIN and Fingerprint ATM authentication modules. In order to come out with a good design and a higher degree of accuracy and correctness, each component of the proposed algorithm for implementing the PIN and fingerprint authentication was designed and tested separately before combining them together, to form a complete system.

4.1 Experimental Analysis

Evaluation and testing of the proposed ATM PIN and fingerprint authentication system was carried with information/data collected from randomly selected, four hundred and fifty student and staff of the Sunyani Polytechnic Sunyani, Ghana. In order to verify if people who have more than one ATM card from a different bank or same bank, turns to use the same PIN for all their ATM cards. A question was asked if respondent uses the same PIN for all their ATM cards, and out of the two hundred and four nine (249) respondents that had more than one ATM card, 159 representing 63.86% answered yes and 93 representing 36.14% answered no.

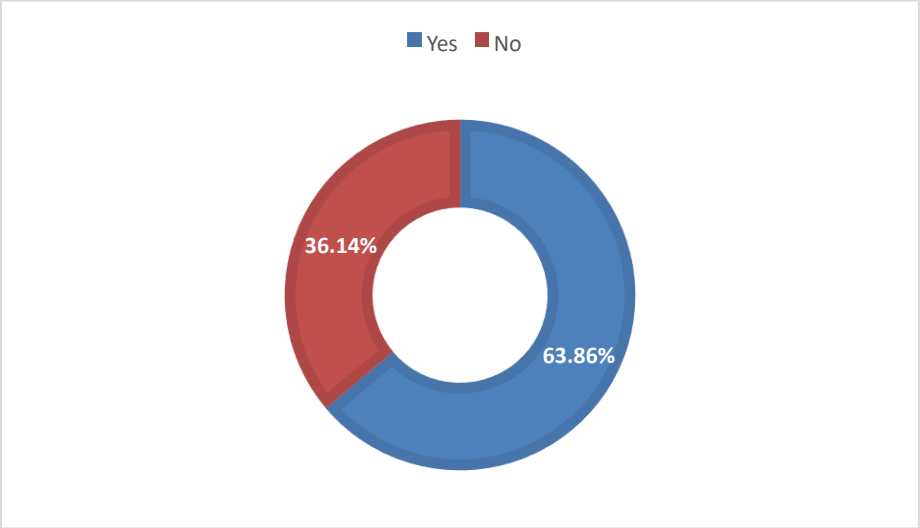

Figure 4.1 Same PIN for two or More ATM Card

4.3 Software Testing

The performance of a biometric system is usually measured in terms of false accept rate (FAR), False rejection rate (FRR) and equal error rate (EER). The false accept rate is the percentage of invalid inputs that are incorrectly accepted (match between input and a non-matching template). The false reject rate is the percentage of valid inputs that are incorrectly rejected (fails to detect a match between input and matching template) (Sainath & Tangellapally, 2010). To test the effectiveness and robustness of the proposed PIN and fingerprint ATM authentication module, two sets of thumbprint data were used for false match rate (FMR) or false acceptance rate (FAR) and False Non-Match Rate (FNMR) or false rejection rate (FRR) testing. Since these indicators are the commonest and simplest indicators for checking the effectiveness, accuracy and performance of fingerprint pattern matching (Iwasokun & Akinyokun, 2013). The first dataset (A) had 1,800 thumbprints, accounting for Four (4) thumbprints collected from the right thumb of each of the

four hundred and fifty (450) respondents. The other dataset (B) also contained the same amount of thumbprints collected from the left thumb of respondents. Datasets (C), (D) and (E) contains 450 thumbprint each from the right thumbs of each subject with different thumb pose for intra-class variation test. All the three thousand, six hundred (3,600) thumbprints from the right and left of respondent were enrolled onto the system for a period of hundred and twenty (120) days , using a digitalpersona (U.are.U 4500) USB fingerprint reader with 512dpi pixel resolution and 18.1mm length by 14.6mm width capturing area. At the initial enrollment stage, some technical and human errors were encountered, these errors were caused by;

1. Incorrect positioning of respondents/subjects thumbs on the scanner.
2. Some moisture effects affecting the scanner platen.
3. Nature of respondents/subject thumb.
4. Working environment (heat).

These problems were resolved as follows, as enrollment progressed, by gathering more technical knowledge on the web.

1. Respondents were guided to position their thumb at the centre of the scanner lens, to give accurate scanning.
2. Restarting the scanner by unplugging and wiping the lens with a clean cotton, wait for some few seconds and plugging it back.
3. Some of the respondents had hardened and rough thumbs which made it a little bit difficult scanning their thumbs, this was resolved by applying a little amount of Vaseline lotion on the thumb, and wipe off after some few seconds to soften the thumb.

4.3.1 Intra-class variations test

The performance of the matching and verification algorithms mostly depends on a different pose variations of the system user thumb or finger on the sensor and something due to deformation of the finger or thumb. To ascertain how the proposed system will react to intra-class variation, each of the four hundred and fifty (450) enrolled templates in the dataset (C) was matched with templates in the dataset (C), (D) and (E) by the same client and the match score recorded. The matching score (also called weights) gives or express the measure of similarity or a distance measure between two minutiae patterns. The greater the score is, the higher is the similarity between them, and for a genuine client the score (S) must be greater than the threshold (T). Figure 4.2 shows a graph of the score obtain from randomly selected 20 fingerprint templates in (C) matched against fingerprint in the dataset (D) and (E) from the same respondent. For the purpose of this research the threshold minimum value was set to thirty (35). The pronouncement of whether a match exists is completed by comparing the matching score (S) to a decision threshold value (T), and if $S \geq T$, then the identity claim is assumed correct.

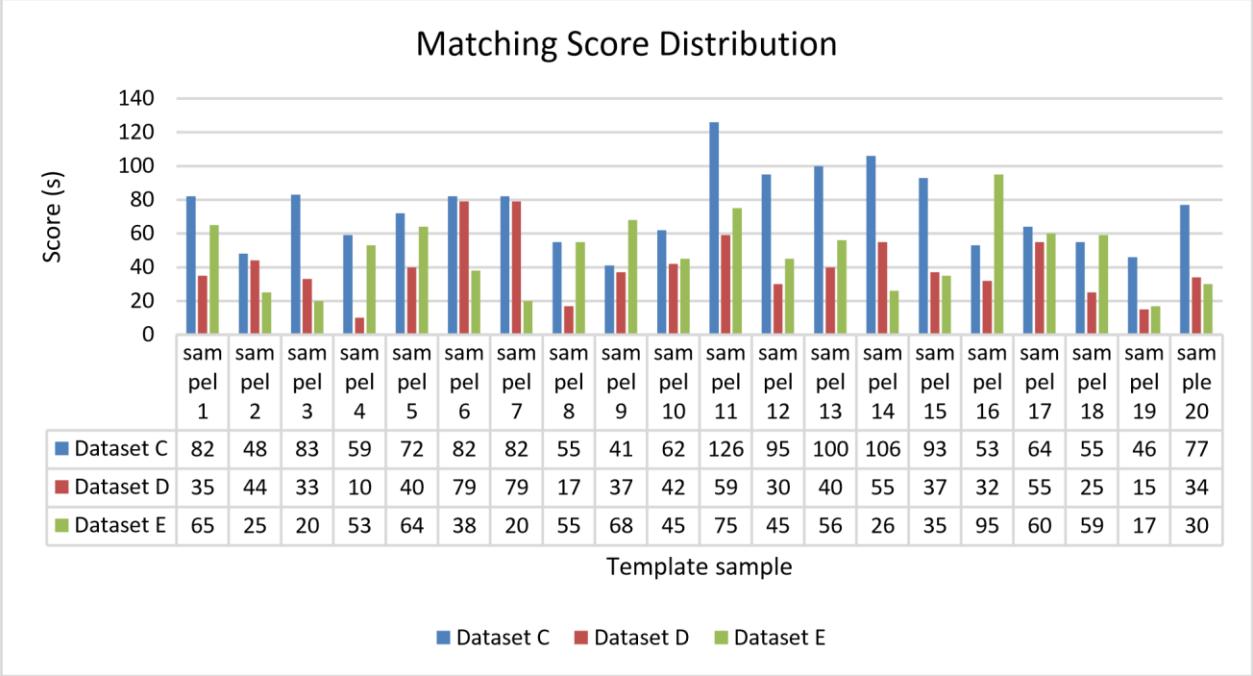

Figure 4.2 Intra-Class Variations Matching Score Distribution

From the bar chart shown in figure 4.2, it can be deduced that the scores obtained by clients differs from dataset to another dataset. These discrepancies in score rate can be attributed to the different poses clients made during the enrollment stage. If clients were to be authenticated with the template stored in dataset D and E, there would have been seven (7) imposters in the dataset (D) and six (6) in the dataset (E) making a total of eleven (13) which equal 65% out of the twenty samples taken at random. From this result, it can be concluded that if client are not guided at the enrolment stage to position their thumbs well on the sensor, there will be a high rate of false rejection at the authentication stage.

4.3.2 False Rejection and False Acceptance Rate

False Rejection Rate

The extracted minutiae are passed via the proposed fingerprint verification module function, which match two minutiae patterns and produce a match score. Experiments were performed and this assumption was deduced; for larger deviances from the correct registration factors we may expect to find local optima. This was also confirmed by experiments. However, the matching score also depends on other factors like softness and hardness of thumb and the positioning of the thumb. In principle, a client score (score of pattern of a person known by the system) should always be higher than the score of impostor. If this would be true, a single threshold, that separates the two groups of scores, could be used to differ between clients and impostors. The equal error rate indicates the accuracy of the system. The false accept rate and false reject rate intersect at a certain point which is called the equal error rate (the point in which the FAR and FRR have the same value). For FAR and FRR testing purpose, three categories of experiments I, K and L were conducted. The first category (I) experiment (FRR test), was carried out on dataset (A), by matching every single thumbprints in dataset (A) with the remaining three other thumbprints from that same thumb in dataset (A), but escaping symmetric matches (i.e., if the template of image f is authenticated against image g, template g is not authenticated against image f); employing the implemented fingerprint matching algorithm. This was to verify the possibility that two match-samples will be acknowledged falsely as unmatched, thus the match score will be lesser than the threshold value.

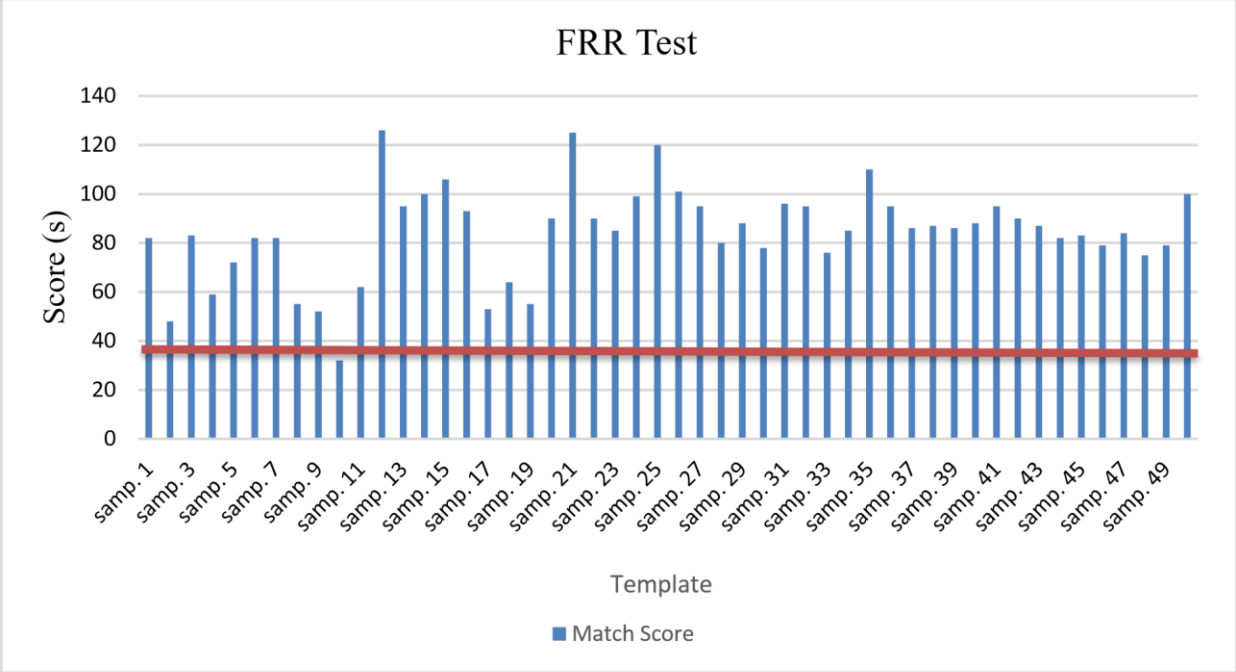

Figure 4.3 False Rejection Rate Score

Figure 4.3 shows an outcome score for randomly picked 50 (templates) samples in the FRR experiment on dataset (A). For a threshold value of 35 it can be realized from the graph in figure 4.3 that, out of the fifty (50) samples, one (1) false reject was accounted. Thus FRR equals (2%) out of 50 as compared with 3.33% out of 30 (Manish, et al., 2011) and 10.57% (Sanjay, et al., 2014), it can be approximated that for all the four hundred and fifty samples that was put under FRR test nine (9) false rejecting will be accounted, making an overall FRR equals nine (9). This means that for every four hundred and fifty clients that visit ATM enhanced with this work, nine are likely to be falsely rejected. The Genuine Acceptance Rate (GAR) is the fraction of genuine scores above the threshold (h). Therefore

$$GAR = 1 - FRR$$

$$1 - 0.02 = 0.98$$

False Acceptance Rate

To determine FAR, the four thumbprints of each thumb, from each respondent in datasets (A) and (B) were matched with the one thousand seven hundred and ninety six (1,796) thumbprints from the 449 remaining respondents' thumbprints at different threshold values. This is to determine the probability that two non-match thumbprints will be mistakenly confirmed as a match.

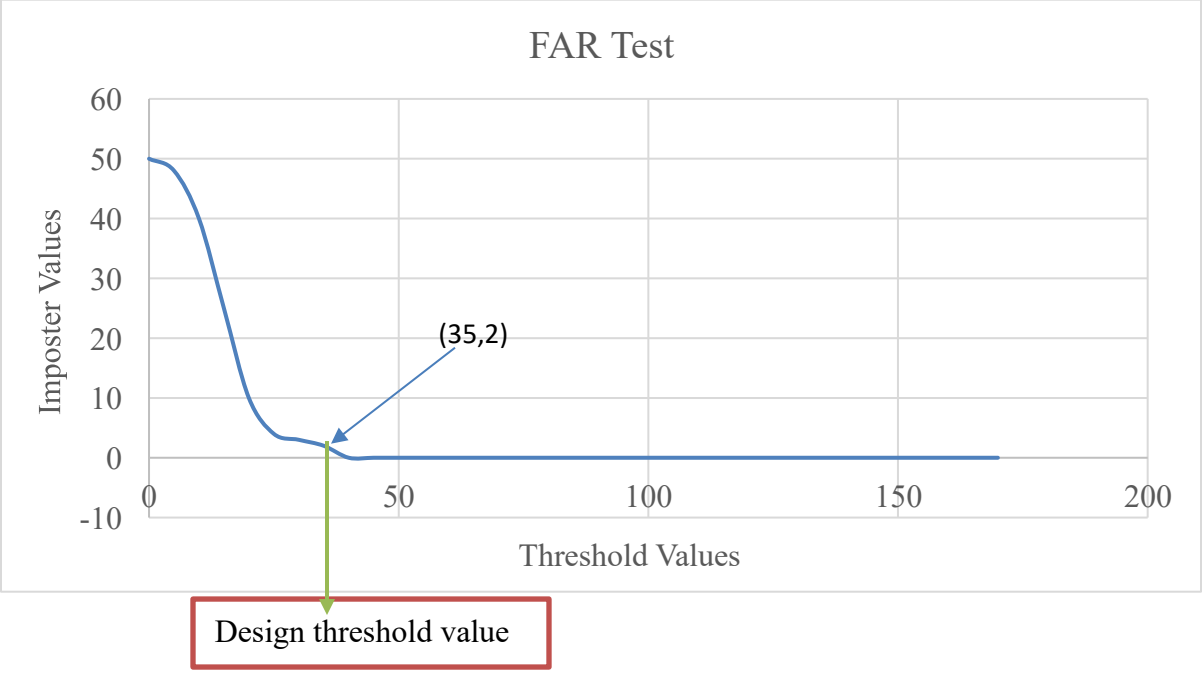

Figure 4.4 False Acceptance Test

Figure 4.4 shows the output curve for the FAR test on dataset (A). From the graph it can be realized that, for a threshold value of thirty-five (35) which is the system set value, two imposter values are recorded as a genuine record out of fifty (50) sample taken at random. Hence FAR equals (4%) for this work as compared to (6.6%) for (Manish, et al., 2011) for 30 samples. In an ideal situation the FAR and FRR should equal zero with the imposter and genuine distributions being disjoint.

Total Error Rate TER which is defined as:

$$TER = \frac{No.\ of\ FAR + No.\ of\ FRR}{Total\ number\ of\ access} - - - (4.1)$$

$$TER = \frac{(2+1)}{50} = 0.06 = 6\%$$

The TER is 6% for a total access of 50 and compared to 13.3% (Manish, et al., 2011) for a total access of 30 and 8.27% (Iwasokun & Akinyokun, 2013).

Figure 4.5 gives the result of the receiver operating characteristic curve (ROC), which demonstrates a true or genuine acceptance rate (1-FRR) plotted against FAR for all thumbprints possible matching thresholds and also a measure of the performance of the entire system on dataset (A).

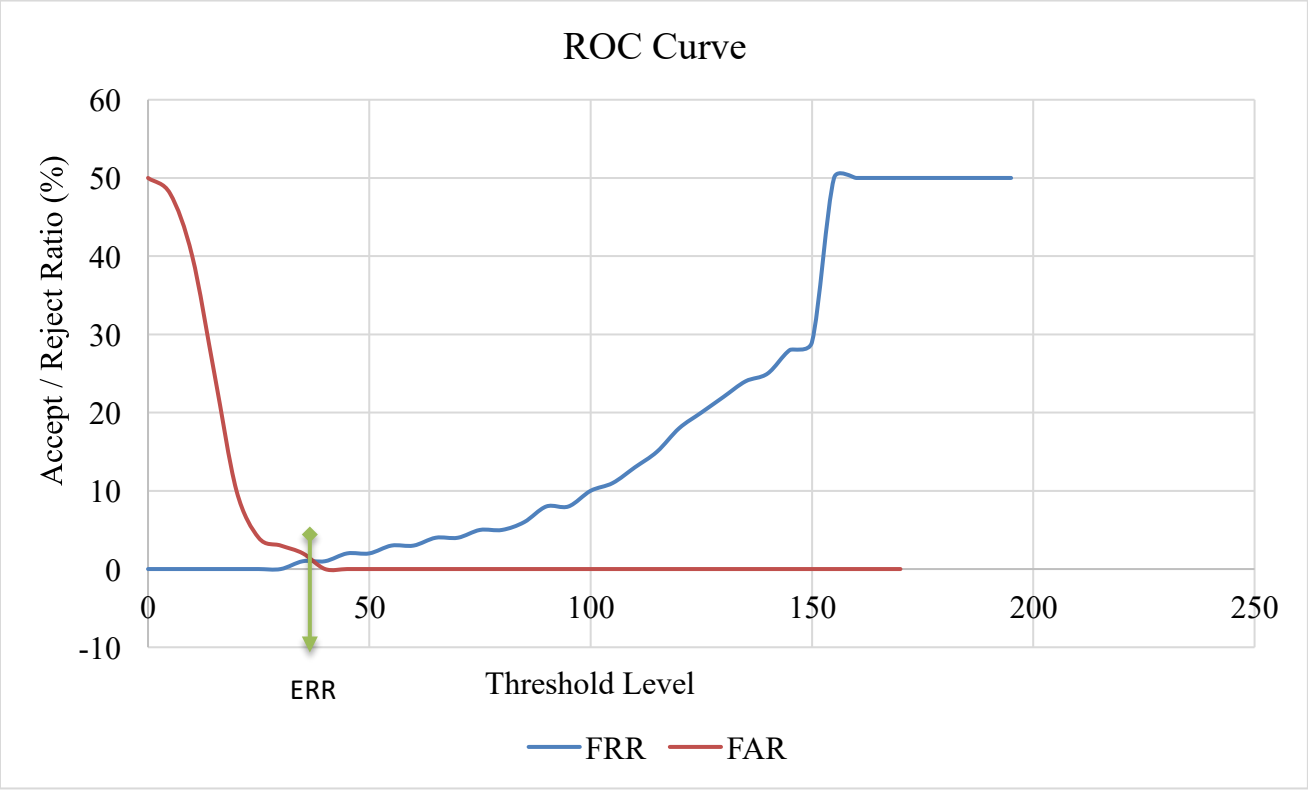

Figure 4.5 ROC Curve for Experiment on Dataset (A)

Every point on the curve shows a particular threshold value. With a TER of 6%, it shows that the developed system is 94% accurate as compared with 89.43% (Sanjay, et al., 2014). The TER and

ROC curve in figure 4.5 shows that the performance of this system depends on the quality of the fingerprint image obtained from the enrollee at the enrollment stage.

Table 4.1 The Average matching time for all three datasets

Dataset	Matching Time (S)
A	1.023
B	1.075
A + B	1.155

Table 4.1 shows the average matching times recorded for all the three categories of experiments performed, thus (I), (K) and (L). A standard deviation of 0.066493107 as compared with 0.0702 (Iwasokun & Akinyokun, 2013) was recorded for the average matching time results of the three sets of experiments, this shows that they are considerably closed. These results, obtained depicts the images equalities in datasets (A) and (B) in terms of qualities, features and resolution/size. The low matching times also indicate that the system is good for identification and verification of individuals at a minimal time.

4.4 Conclusion

This worked focused on the use of a fingerprint in addition to the normal PIN to formulate a very strong, secure and dependable identification and verification system to boost ATM security. The key purpose for introducing biometric in ATM systems is to enhance the overall security.

Biometrics give greater security and ease than traditional methods of personal recognition (Khan, 2010). The recorded values of FAR, FRR, TER and ROC curve indicates that, the proposed system is a well secured system for providing a strong technique for checkmating the activities of system invaders/imposters as well as providing smooth and reliable access for genuine users.

Chapter 5

CONCLUSIONS AND RECOMMENDATIONS

5.0 Introduction

This chapter presents the recommendation and conclusions of this research.

5.1 Conclusion

The conclusions arising out of this research, based on the findings, are given below.

- The proposed fingerprint and PIN system has an overall efficiency of 94%, FAR 4%, FRR 2%, TER 6% and GAR 98%. Compared to other fingerprint identification and verification systems, the proposed system provides an improved performance in matching time and partial elimination of false minutiae from its fingerprint database.

- The FRR can be reduced if at the enrollment stage clients/customers are well guided to position their thumbs well on the fingerprint scanner.

- The proposed system is a good cost effective measure for implementing a well secure ATM transactions to protect ATM users from fraudsters.

5.2 Recommendation

The recommendations of this research could be summarized as follows:

- Decision-makers need to appreciate the level of security assured through the usage of biometric systems and the transformation that can exist between the perception and the authenticity of the sense of security delivered.

- The Bank of Ghana (BoG) and the Ghana Association of Bankers (GAB) which has the mandate to implement strategic actions in the banking sector of Ghana should pilot the installation of ATM enhanced with this system as a cost reduction strategy and security for their customers and clients.

- The great difference obtained on *Intra -class* variations test in this research indicates that, if clients thumb pose at enrollment do not match with thumb pose at verification, a falsehood rejection will occur. Hence the Electoral commission (EC) of Ghana should ensure that, the thumbs of voters at enrollment and voting days are positioned well on the fingerprint scanner, to prevent false rejection, causing confusion at voting days.

- Experimental validation should be conducted to confirm the results presented in this research work.

- Future work should look at reducing the Total Error Rate (TER) via integrated and optimized algorithms and also a combination of fingerprint and other biometrics such as the face and voice for the identification and verification of ATM users.

REFERENCES

1. Adams, A. & Sasse, M. A., 1999. Users are Not the Enemy. Commun.. *ACM 42, 12,* pp. 40-46.
2. Agarwal, T., 2010. *How ATMs Work.* [Online]
   Available at: http://www.elprocus.com/automatic-teller-machine-types-workingadvantages
   [Accessed 5 January 2015].
3. Akinyemi, I., Omogbadegun, Z. & Oyelami, O., 2010. Towards Designing a Biometric Measure for Enhancing ATM Security in Nigeria EBanking System.. *International Journal of Electrical & Computer Sciences IJECS-IJENS 10,* pp. 68-73.
4. Anand, D. A., Dinesh, G. & Naveen, H. D., 2013. A Reliable ATM Protocol and

Comparative Analysis on Various Parameters with other ATM Protocols. *International Jouranl of Communication and Computer Technologies (IJCCT), ISSN: 2278-9723,* 01(56), pp. 192-197.

5. Anil , K., Jianjiang , F. & Karthik , N., 2010. Fingerprint Matching. *IEEE Computer Society,* pp. 36-44.
6. APCA, 2014. *Australian payments fraud details and Data ,* Australia: s.n.
7. Babatunde, I. G., Akinyokun , C. O. & Olatunbosun, O., 2012. A Mathematical Modeling Method for Fingerprint Ridge Segmentation and Normalization. *International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555,* II(02), pp. 263-267.
8. Batiz-Lazo, B. & Barrie, . A., 2005. *The business and technology history of automated teller machine in the UK.* London, Queen Mary University, pp. 1-10.
9. BBC , 2011. *News.* [Online]
   Available at: http://www.bbc.com/news/uk-england-london-12655833
   [Accessed 7 July 2015].
10. Bhosale, S. T. & Sawant, D. B. ,., 2012. Security in E-Banking via Card Less Biometric ATMs. *International Journal of Advanced Technology & Engineering Research (IJATER),* p. Volume 2.
11. Bianchi, A., Oakley, I. & Kwon, D. S., 2010. *The secure haptic keypad: a tactile password system..* s.l., ACM, pp. 1089-1092..
12. Bond , M. & Zielinski, P., 2004. *Encrypted? Randomised? Compromised? (When cryptographically secured data is not secure).* Gold Coast, Australia, s.n.

13. Burelli, F., Gorelikov, A. & Labianca, M., 2014. *ATM Benchmarking Study 2014 and Industry Report,* London SW1P 3HQ, UK: Value Partners Management Consulting Ltd Kings Buildings, 7th Floor,16 Smith Square.
14. Chakrabarty, K. C., 2013. *Fraud in the banking sector – causes, concerns and cures.* New Delhi, ASSOCHAM, pp. 1-13.
15. Cynthia, B., 2000. *The measurement of white-collar crime using Uniform Crime,* New York: Reporting (UCR) Data. S department of Justice, Federal Bureau of Investigation.
16. Daniel, B., 2011. [Online] Available at: http://www.guardianseries.co.uk/news/wfnews/8946110.CHINGFORD___Cash_machine_fraudsters__arreste d/ [Accessed 7 July 2015].
17. Dare, T., 2011. *ATM Security annual report,* Nigeria: NCR .
18. Das, S. & Jhunu, D., 2011. Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System. *International Journal of Information and Communication Technology Research,* pp. 197-203.
19. Diebold, I., 2002 . *ATM fraud and security: White Paper,* New York: s.n.
20. Fahmida, Y. R., 2013. *Security Week.* [Online] Available at: http://www.securityweek.com/exclusive-new-malware-targeting-possystems-atms-hits-major-usbanks?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Securityw ee k+(SecurityWeek+RSS+Feed)&utm_content=Google+Reader [Accessed 24 June 2015].
21. Gazal, B. & Ranjeet, K. S., 2014. Fingerprints in Automated Teller Machine-A Survey.

Volume-3, April, pp. 1-4.

22. Gunn, L., 2010. *European ATM crime report. Technical Report 1.2,* s.l.: European ATM Security Team (EAST),.
23. Han, F. et al., 2006. *A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications.* Hong Kong, China, Springer Berlin Heidelberg, pp. 675681.
24. Hirakawa, Y., 2013. Random Board: Password Authentication Method with Tolerance to Video-Recording Attacks. *International Journal of Innovation, Management and Technology, Vol. 4, No. 5,* pp. 455-460.
25. Ihejiahi, R., 2009. How to fight ATM fraud online. *Nigeria Daily News, June 21,* p. P. 18.
26. Iwasokun, G., Akinyokun, O., Alese, B. & Olabode, O., 2012. Fingerprint image enhancement: Segmentation to thinning.. *International Journal of Advanced Computer Science and Applications Indian 3,* pp. 50-89.
27. Iwasokun, G. B. & Akinyokun, O. C., 2013. A Fingerprint-based Authentication Framework for ATM Machines. *Journal of Computer Engineering & Information Technology,* pp. 1-8.
28. Jegede, C. A., 2014. Effects of Automated Teller Machine on the Performance of Nigerian Banks. *American Journal of Applied Mathematics and Statistics 2 (1),* pp. 40-46.
29. Jermyn, I. et al., 1999. *The design and analysis of graphical passwords..* s.l., USENIX Association, pp. 1-1.
30. Khan, H. Z. U., 2010. Comparative Study of Authentication Techniques. *International Journal of Video& Image Processing and Network Security IJVIPNS-IJENS ,* 10(4), pp. 9-13.

31. Kitten, T., 2015. [Online]

Available at: http://www.bankinfosecurity.com/blogs/easy-access-fuels-atm-attacks-p-1884

[Accessed 7 July 2015].

32. Klokova, A., 2011. *Comparison of various biometric methods,* Southampton, UK, SO17 1BJ: Electronics and Computer Science University of Southampton University Road.

33. Krebs, B., 2010. *ATM Skimmers Part II.* [Online]

Available at: http://krebsonsecurity.com/2010/02/atm-skimmers-part-ii/

[Accessed 24 June 2015].

34. Krebs, B., 2010. *Would You Have Spotted the Fraud.* [Online] Available at: http://krebsonsecurity.com/all-about-skimmers/

[Accessed 24 June 2015].

35. Lalzirtira, 2013. *Graphical User Authentication,* India: Department of Computer Science and Engineering National Institute of Technology Rourkela.

36. Lavanya, K. & Raju, C. N., 2013. A Comparative Study on ATM Security with Multimodal Biometric System. *International Journal of Computer Science & Engineering Technology (IJCSET),* IV(06), pp. 808-812.

37. Luca, A., 2011. *Designing Usable and Secure Authentication Mechanisms For Public Spaces (Doctoral dissertation, lmu),* s.l.: s.n.

38. Madu, C. & Madu, A., 2002. Dimensions of e-quality. *International Journal of Quality & Reliability Management, 19(3),* pp. 246-58.

39. Mandal, S., 2013. A Review on Secured Money Transaction with Fingerprint Technique in ATM System. *International Journal of Computer Science and Network,* 2(4), pp. 8-11. 40. Manish, . M., Ajit , S. K., Thakur, S. S. & Sinha, D., 2011. Secure Biometric

Cryptosystem for Distributed System. *International Journal Communication & Network Security (IJCNS),* Volume-I(Issue-II), pp. 28-32.

41. Modernghana, 2013. *Modernghana.* [Online]
Available at: http://www.modernghana.com/news/463043/1/hackers-steal-45-million-inatm-card-scam-federal.html
[Accessed 10 June 2015].
42. Mohammed, L. A., 2011. *Use of biometrics to tackle ATM fraud..* Malaysia,, IACSIT Press, Kuala Lumpur, pp. 331-335.
43. Mohsin, K., Saifali, K., Sharad, O. & Dr.D.R.Kalbanded, 2015. *Enhanced security for ATM machine with OTP and Facial.* s.l., Elsevier B.V., pp. 390-396.
44. Mudholkar , S. S., Shende , P. M. & Sarode, M. V., 2012. Biometric Authentication Techhniques for Intrusion Detection System Using Fingerprint Recogbition. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT),* pp. 57-65.
45. Myo, N., 2009. Fingerprint Identification Based on the Model of the Outer Layers of Polygon Subtraction. *International Conference on Education Technology and Computer,* p. 201 – 204.
46. Ndife, .. A., Ifesinachi, .. E., Anthony, .. O. & Davies, .. ,., 2013. An Enhanced Technique in ATM Risk Reduction using Automated. *Volume No.4*, 06 June , pp. 1132-1138.
47. Obiano, W., 2009. *How to fight ATM fraud Online,* Nigeria: Daily News, June 21, P. 18.
48. Obour, S. K., 2013. [Online]
Available at: http://graphic.com.gh/news/general-news/8459-gcb-confirms-money-theftfrom-atm-but-says-amount-is-lower-than-gh-3-million.html
49. Omari, R. K. B., 2012. *An assessment of the use of Automated Teller Machine (A.T.M) of*

Barclays Bank Ghana Limited Akim Oda Branch, Akim Oda: s.n.

50. Onyesolu, M. O. & Ezeani, I. M., 2012. ATM Security Using Fingerprint Biometric Identifer: An Investigative Study. *International Journal of Advanced Computer Science and Applications, Vol. 3, No.4,* pp. 68-72.
51. Passfaces, Corporation, 2005. [Online]
    Available at: http://www.realuser.com/enterprise/about/about_passfaces.htm
    [Accessed 9 July 2015].
52. Rasiah, D., 2010. ATM Risk Management and Controls. *European Journal of Economics, Finance and Administrative Sciences , 21, ,* 2014 January.pp. 161-171.
53. Ratha, N., Connell, J. & Bolle, R., 2001. Enhancing Security and Privacy in Biometricsbased Authentication Systems. *IBM Systems Journal, vol. 40, no. 3,* pp. 614-634.
54. Roth, V., Richter, K. & Freidinger, R., 2004. A Pin-Entry Method Resilient Against Shoulder Surfing. pp. 236-245.
55. Sainath , M. & Tangellapally , R. S., 2010. *Implementation and Evaluation of NIST Biometric Image Software for Fingerprint Recognition,* Sweden : Blekinge Institute of Technology.
56. Sanjay, S. G. et al., 2014. ATM Transaction Security System Using Biometric Palm Print Recognition and Transaction Confirmation System. *International Journal Of Engineering And Computer Science,* pp. 5332-5335.
57. Santhi, B. & Kumar, R., 2012. Novel Hybrid Technology in ATM Security Using Biometrics. *Journal of Theoretical and Applied Information Technology,* pp. 217-223.

58. Saropourian, B., 2009. A new approach of finger-print recognition based on neural network," Computer Science and Information Technology, 2009. ICCSIT 2009. *ICCSIT 2009. 2nd IEEE International Conference ,* pp. 158-161.

59. Shaikh, S. A. & Rabaiotti, J. R., 2010. Characteristic trade-offs in designing large-scale biometric-based identity management systems. *Journal of Network and Computer Applications vol. 33,* p. 342–351.

60. SpiderLabs, 2012. *Trustwave Holdings Inc..* [Online] Available at: https://www.trustwave.com/Company/SpiderLabs/ [Accessed 07 May 2015].

61. Subh , M. & Vanithaasri , S., 2012. A Study on Authenticated Admittance of. *International Journal of Advances in Engineering & Technology 4,* pp. 456-463.

62. Susmita, M., 2013. A Review on Secured Money Transaction with Fingerprint Technique in ATM System. *International Journal of Computer Science and Network, Volume 2, Issue 4,* pp. 8-11.

63. Takada, . T., 2008. FakePinter: The authentication technique which has tolerance to video recording attacks. *Information processing society of Japan (IPSJ) transaction, vol. 49, no. 9,* pp. 3051-3061.

64. Tedder, K., 2009. *A Review of Fraud Costs and Trends,* s.l.: s.n.

65. Thai, R., 2003. *Fingerprint Image Enhancement and Minutiae Extraction, PhD Thesis Submitted to School of Computer Science and Software Engineering,* Australia: University of Western .

66. Wheatley, M., 2013. *Silicon Angle.* [Online] Available at: http://siliconangle.com/blog/2013/04/01/new-malware-goes-for-the-moneyinfects-atms-cash-registers/

[Accessed 24 June 2015].

67. Zhao, H. & Li, X., 2007. “S3PAS: A Scalable Shoulder-Surfing Resistant Textualgraphical Password Authentication Scheme. *IEEE Advanced Information Networking and Applications Workshops,* pp. 467-472.

APPENDIX A

FINGERPRINT ENROLLMENT, VERIFICATION AND IDENTIFICATION CODES

```
using GrFingerXLib; using System;
using System.Windows.Forms; using
System.Runtime.InteropServices; using
System.Data.SqlClient;

// Raw image data type. public
struct TRawImage
{
   // Image data.
   public object img;
// Image width.
public int width;     //
Image height.
public int height;     //
Image resolution.
   public int Res;
};

public class Util
{

   // Some constants to make our code cleaner
public const int ERR_CANT_OPEN_BD = -999;
public const int ERR_INVALID_ID = -998;
   public const int ERR_INVALID_TEMPLATE = -997;
```

```
    // ------------------------------------------------------------------------------
    // Support functions
    // ------------------------------------------------------------------------------

    // This class creates an Util class with some functions
// to help us to develop our GrFinger Application
public Util(ListBox lbLog, PictureBox pbPic,
        Button btEnroll, Button btnExtract, Button btIdentify, Button btVerify,
        CheckBox cbAutoExtract, CheckBox cbAutoIdentify)
    {
        _lbLog = lbLog;
        _pbPic = pbPic;
        _btEnroll = btEnroll;
        _btExtract = btnExtract;
        _btIdentify = btIdentify;
        _btVerify = btVerify;
        _cbAutoExtract = cbAutoExtract;
        _cbAutoIdentify = cbAutoIdentify;
        _DB = null;
        _tpt = null;
        _consolidatedTpt = null;
    }

    //



    ~Util()
    {
    }
    //    Write a message in log box.
public void WriteLog(String msg)
    {
        _lbLog.Items.Add(msg);
        _lbLog.SelectedIndex = _lbLog.Items.Count - 1;
        _lbLog.ClearSelected();
    }
    // Write and describe an error.
    public void WriteError(GrFingerXLib.GRConstants errorCode)
    {
        switch ((int)errorCode)
        {
            case (int)GRConstants.GR_ERROR_INITIALIZE_FAIL:
                WriteLog("Fail to Initialize GrFingerX. (Error:" + errorCode + ")");
return;             case (int)GRConstants.GR_ERROR_NOT_INITIALIZED:
```

```
            WriteLog("The GrFingerX Library is not initialized. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_FAIL_LICENSE_READ:
            WriteLog("License not found. See manual for troubleshooting. (Error:" + errorCode +
")");
            MessageBox.Show("License not found. See manual for troubleshooting.");
return;         case (int)GRConstants.GR_ERROR_NO_VALID_LICENSE:
            WriteLog("The license is not valid. See manual for troubleshooting. (Error:" + errorCode
+ ")");
            MessageBox.Show("The license is not valid. See manual for troubleshooting.");
return;         case (int)GRConstants.GR_ERROR_NULL_ARGUMENT:
            WriteLog("The parameter have a null value. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_FAIL:
            WriteLog("Fail to create a GDI object. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_ALLOC:
            WriteLog("Fail to create a context. Cannot allocate memory. (Error:" + errorCode +
")");             return;          case
(int)GRConstants.GR_ERROR_PARAMETERS:
            WriteLog("One or more parameters are out of bound. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_WRONG_USE:
            WriteLog("This function cannot be called at this time. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_EXTRACT:
            WriteLog("Template Extraction failed. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_SIZE_OFF_RANGE:
            WriteLog("Image is too larger or too short.  (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_RES_OFF_RANGE:
            WriteLog("Image have too low or too high resolution. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_CONTEXT_NOT_CREATED:
            WriteLog("The Context could not be created. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_INVALID_CONTEXT:
            WriteLog("The Context does not exist. (Error:" + errorCode + ")");
return;

        // Capture error codes

        case (int)GRConstants.GR_ERROR_CONNECT_SENSOR:
            WriteLog("Error while connection to sensor. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_CAPTURING:
            WriteLog("Error while capturing from sensor. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_CANCEL_CAPTURING:
            WriteLog("Error while stop capturing from sensor. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_INVALID_ID_SENSOR:
            WriteLog("The idSensor is invalid. (Error:" + errorCode + ")");
return;         case
(int)GRConstants.GR_ERROR_SENSOR_NOT_CAPTURING:
            WriteLog("The sensor is not capturing. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_INVALID_EXT:
```

```
            WriteLog("The File have a unknown extension. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_INVALID_FILENAME:
            WriteLog("The filename is invalid. (Error:" + errorCode + ")");
return;         case
(int)GRConstants.GR_ERROR_INVALID_FILETYPE:
            WriteLog("The file type is invalid. (Error:" + errorCode + ")");
return;         case (int)GRConstants.GR_ERROR_SENSOR:
            WriteLog("The sensor raise an error. (Error:" + errorCode + ")");
return;

          // Our error codes
          case ERR_INVALID_TEMPLATE:
            WriteLog("Invalid Template. (Error:" + errorCode + ")");
return;         case ERR_INVALID_ID:
            WriteLog("Invalid ID. (Error:" + errorCode + ")");
return;         case ERR_CANT_OPEN_BD:
            WriteLog("Unable to connect to DataBase. (Error:" + errorCode + ")");
return;

default:
            WriteLog("Error:"     +     errorCode);
return;
        }
    }

    // Check if we have a valid template
    private bool TemplateIsValid()
    {
        // Check the template size and data
        return ((_tpt._size > 0) && (_tpt._tpt != null));
    }

    // Check if we have a valid template
    private bool ConsolidatedTemplateIsValid()
    {
        // Check the template size and data
        return ((_consolidatedTpt._size > 0) && (_consolidatedTpt._tpt != null));
    }

    // -------------------------------------------------------------------------
    // Main functions for fingerprint recognition management
    // -------------------------------------------------------------------------

    // Initializes GrFinger ActiveX and all necessary utilities.
```

```
   public int InitializeGrFinger(AxGrFingerXLib.AxGrFingerXCtrl grfingerx)
   {
      GRConstants result;

      _grfingerx = grfingerx;
//Check DataBase Class.        if
(_DB == null)            _DB =
new DBClass();        //Open
DataBase        if
(_DB.openDB() == false)
      {
         return ERR_CANT_OPEN_BD;
      }

      //Create a new Template
if (_tpt == null)
         _tpt = new TTemplate();

      //Create a new consolidated template
if (_consolidatedTpt == null)
         _consolidatedTpt = new TTemplate();

      //Create a new raw image
      _raw = new TRawImage();

      //Initialize library
      result = (GRConstants)_grfingerx.Initialize();
      if (result < 0) return (int)result;
      return (int)_grfingerx.CapInitialize();
   }
   //  Finalizes library and close DB.
   public void FinalizeUtil()
   {
      // finalize library
      _grfingerx.Finalize();
      _grfingerx.CapFinalize();
      // close DB
      _DB.closeDB();
      _raw.img = null;
      _tpt = null;
      _consolidatedTpt = null;
      _DB = null;
   }
```

```
   // Display fingerprint image on screen
   public void PrintBiometricDisplay(bool isBiometric, GrFingerXLib.GRConstants contextId)
   {
      // handle to finger image
      System.Drawing.Image handle = null;
      // screen HDC
      IntPtr hdc = GetDC(System.IntPtr.Zero);

      if (isBiometric)
      {
         // get image with biometric info
         _grfingerx.BiometricDisplay(ref _tpt._tpt,
            ref  _raw.img,  _raw.width,  _raw.height,  _raw.Res,  hdc.ToInt32(),
ref handle, (int)contextId);
      }
else
      {
         // get raw image
         _grfingerx.CapRawImageToHandle(ref _raw.img, _raw.width,
            _raw.height, hdc.ToInt32(), ref handle);
      }

      // draw image on picture box
      if (handle != null)
      {
         _pbPic.Image = handle;
         _pbPic.Update();
      }

      // release screen HDC
      ReleaseDC(System.IntPtr.Zero, hdc);
   }

   //display finger to
   public void PrintBiometricDisplay(bool isBiometric, GrFingerXLib.GRConstants
contextId,System.Windows.Forms.PictureBox _pbPic)
   {
      // handle to finger image
      System.Drawing.Image handle = null;
      // screen HDC
      IntPtr hdc = GetDC(System.IntPtr.Zero);

      if (isBiometric)
      {
```

```
        // get image with biometric info
        _grfingerx.BiometricDisplay(ref _tpt._tpt,
            ref _raw.img, _raw.width, _raw.height, _raw.Res, hdc.ToInt32(),
ref handle, (int)contextId);
      }
else
      {
        // get raw image
        _grfingerx.CapRawImageToHandle(ref _raw.img, _raw.width,
            _raw.height, hdc.ToInt32(), ref handle);
      }

      // draw image on picture box
      if (handle != null)
      {
        _pbPic.Image = handle;
        _pbPic.Update();
      }

      // release screen HDC
      ReleaseDC(System.IntPtr.Zero, hdc);
   }

   public void PrintBiometricDisplay1(bool isBiometric, GrFingerXLib.GRConstants contextId,
System.Windows.Forms.PictureBox _pbPic, TTemplate _tpt)
   {
      // handle to finger image
      System.Drawing.Image handle = null;
      // screen HDC
      IntPtr hdc = GetDC(System.IntPtr.Zero);

      if (isBiometric)
      {
        // get image with biometric info
        _grfingerx.BiometricDisplay(ref _tpt._tpt,
            ref _raw.img, _raw.width, _raw.height, _raw.Res, hdc.ToInt32(),
ref handle, (int)contextId);
      }
else
      {
        // get raw image
        _grfingerx.CapRawImageToHandle(ref _raw.img, _raw.width,
            _raw.height, hdc.ToInt32(), ref handle);
      }
```

```
      // draw image on picture box
      if (handle != null)
      {
         _pbPic.Image = handle;
         _pbPic.Update();
      }

      // release screen HDC
      ReleaseDC(System.IntPtr.Zero, hdc);
   }
   // Add a consolidated fingerprint template to database
string AcctNo, CustomerID, PIN;
   public int Enroll()
   {        int id
= 0;
      // Checks if template is valid.
      if (ConsolidatedTemplateIsValid())
      {
         // Adds template to database and returns template ID.
         _DB.addTemplate(_consolidatedTpt, AcctNo, CustomerID, PIN, ref id);
return id;
      }
else       {
         return -1;
      }
   }

   // Extract a fingerprint template from current image
public int ExtractTemplate()
   {
      int result;

      // set current buffer size for the extract template
      _tpt._size = (int)GRConstants.GR_MAX_SIZE_TEMPLATE;
      result = (int)_grfingerx.Extract(
         ref _raw.img, _raw.width, _raw.height, _raw.Res,
ref _tpt._tpt, ref _tpt._size,
         (int)GRConstants.GR_DEFAULT_CONTEXT);
      // if error, set template size to 0
      if (result < 0)
      {
         // Result < 0 => extraction problem
         _tpt._size = 0;
```

```
        }
        return result;
    }

    // Identify current fingerprint on our database
public string _AcctNo, _CustomerID, _PIN;
    public int ID = 0;
    public int Identify(ref int score , string accno,string pin)
    {
        GRConstants result;
        int id;
        SqlDataReader rs;
        TTemplate tptRef;

        // Checking if template is valid.
        if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;
// Starting identification process and supplying query template.
result = (GRConstants)_grfingerx.IdentifyPrepare(ref _tpt._tpt,
(int)GRConstants.GR_DEFAULT_CONTEXT);
        // error?
        if (result < 0) return (int)result;
        // Getting enrolled templates from database.
rs = _DB.getTemplates();        while (rs.Read())
        {
            // Getting current template from recordset.
tptRef = _DB.getTemplate(rs);            AcctNo =
rs.GetString(0);
            _CustomerID = rs.GetString(2);
            _PIN = rs.GetString(3);
            ID = rs.GetInt32(4);
            // Comparing current template.
            result = (GRConstants)_grfingerx.Identify(ref tptRef._tpt, ref score,
(int)GRConstants.GR_DEFAULT_CONTEXT);

            // Checking if query template and the reference template match.
            if (result == GRConstants.GR_MATCH && AcctNo == accno && pin ==_PIN )
            {
                id = _DB.getId(rs);
                rs.Close();
return id;
            }
            else if (result < 0)
            {
```

```
            rs.Close();
return (int)result;
          }
              }
       // Closing recordset.
       rs.Close();
       return (int)GRConstants.GR_NOT_MATCH;
   }


   //idenfiy
   public int Identify(ref int score)
   {
      GRConstants result;
      int id;
      SqlDataReader rs;
      TTemplate tptRef;

      // Checking if template is valid.
      if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;
// Starting identification process and supplying query template.
result = (GRConstants)_grfingerx.IdentifyPrepare(ref _tpt._tpt,
(int)GRConstants.GR_DEFAULT_CONTEXT);
      // error?
      if (result < 0) return (int)result;
      // Getting enrolled templates from database.
rs = _DB.getTemplates();
      while (rs.Read())
      {
         // Getting current template from recordset.
tptRef = _DB.getTemplate(rs);            AcctNo =
rs.GetString(0);
         _CustomerID = rs.GetString(2);
_PIN = rs.GetString(3);           //
Comparing current template.
         result = (GRConstants)_grfingerx.Identify(ref tptRef._tpt, ref score,
(int)GRConstants.GR_DEFAULT_CONTEXT);

         // Checking if query template and the reference template match.
         if (result == GRConstants.GR_MATCH)
         {
            id = _DB.getId(rs);
rs.Close();              return
id;
         }
```

```
        else if (result < 0)
        {
rs.Close();             return
(int)result;          }
      }
      // Closing recordset.
      rs.Close();
      return (int)GRConstants.GR_NOT_MATCH;
   }


   //identify thumb B
   public int IdentifyB(ref int score)
   {
      GRConstants result;
      int id;
      SqlDataReader rs;
      TTemplate tptRef;

      // Checking if template is valid.
      if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;
// Starting identification process and supplying query template.
result = (GRConstants)_grfingerx.IdentifyPrepare(ref _tpt._tpt,
(int)GRConstants.GR_DEFAULT_CONTEXT);
      // error?
      if (result < 0) return (int)result;
      // Getting enrolled templates from database.
rs = _DB.getTemplatesB();       while
(rs.Read())
      {
         // Getting current template from recordset.
tptRef = _DB.getTemplate(rs);          AcctNo =
rs.GetString(0);
         _CustomerID = rs.GetString(2);
_PIN = rs.GetString(3);          //
Comparing current template.
         result = (GRConstants)_grfingerx.Identify(ref tptRef._tpt, ref score,
(int)GRConstants.GR_DEFAULT_CONTEXT);

         // Checking if query template and the reference template match.
         if (result == GRConstants.GR_MATCH)
         {
            id = _DB.getId(rs);
rs.Close();             return
id;
```

```
            }
            else if (result < 0)
            {
               rs.Close();
return (int)result;
            }
         }


         // Closing recordset.
         rs.Close();
         return (int)GRConstants.GR_NOT_MATCH;
      }

      //VERIFY C

      public int IdentifyC(ref int score)
      {
         GRConstants result;
         int id;
         SqlDataReader rs;
         TTemplate tptRef;

         // Checking if template is valid.
         if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;
// Starting identification process and supplying query template.
result = (GRConstants)_grfingerx.IdentifyPrepare(ref _tpt._tpt,
(int)GRConstants.GR_DEFAULT_CONTEXT);
         // error?
         if (result < 0) return (int)result;
         // Getting enrolled templates from database.
rs = _DB.getTemplatesC();         while
(rs.Read())
         {
            // Getting current template from recordset.
tptRef = _DB.getTemplate(rs);            AcctNo =
rs.GetString(0);
            _CustomerID = rs.GetString(2);
_PIN = rs.GetString(3);            //
Comparing current template.
            result = (GRConstants)_grfingerx.Identify(ref tptRef._tpt, ref score,
(int)GRConstants.GR_DEFAULT_CONTEXT);

            // Checking if query template and the reference template match.
if (result == GRConstants.GR_MATCH)
```

```
            {
               id = _DB.getId(rs);
rs.Close();                return
id;
            }
            else if (result < 0)
            {
rs.Close();                return
(int)result;
            }
         }


         // Closing recordset.
         rs.Close();
         return (int)GRConstants.GR_NOT_MATCH;
      }

      public string  FARID = "";
//idenfiy for FAR test     public int
IdentifyF(ref int score)
      {
         GRConstants result;
         int id;
         SqlDataReader rs;
         TTemplate tptRef;

         // Checking if template is valid.
         if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;
// Starting identification process and supplying query template.
result = (GRConstants)_grfingerx.IdentifyPrepare(ref _tpt._tpt,
(int)GRConstants.GR_DEFAULT_CONTEXT);
         // error?
         FARID = "";         if (result < 0)
return (int)result;
         // Getting enrolled templates from database.
rs = _DB.getTemplates();
         while (rs.Read())
         {
            // Getting current template from recordset.
            tptRef       =       _DB.getTemplate(rs);
AcctNo = rs.GetString(0);
            _CustomerID = rs.GetString(2);
            _PIN = rs.GetString(3);
            ID = rs.GetInt32(4);
```

```
        // Comparing current template.
FARID = _CustomerID;
        result = (GRConstants)_grfingerx.Identify(ref tptRef._tpt, ref score,
(int)GRConstants.GR_DEFAULT_CONTEXT);

        // Checking if query template and the reference template match.
if (result == GRConstants.GR_MATCH)
        {
           id = _DB.getId(rs);
rs.Close();             return
id;
        }
        else if (result < 0)
        {
rs.Close();             return
(int)result;
        }
      }
      // Closing recordset.
      rs.Close();
      return (int)GRConstants.GR_NOT_MATCH;
   }

   // Check current fingerprint against another one in our database
   public int Verify(int id, ref int score)
   {
      TTemplate tptRef;

      // Checking if template is valid.
      if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;

      // Getting template with the supplied ID from database.
tptRef = _DB.getTemplate(id);

      // Checking if ID was found.             if
((tptRef._tpt == null) || (tptRef._size == 0))
      {
         return ERR_INVALID_ID;
      }
      // Comparing templates.
      return (int)_grfingerx.Verify(ref _tpt._tpt, ref tptRef._tpt,
         ref score, (int)GRConstants.GR_DEFAULT_CONTEXT);
   }
```

```
   public int VerifyB(int id, ref int score)
   {
      TTemplate tptRef;

      // Checking if template is valid.
      if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;

      // Getting template with the supplied ID from database.
tptRef = _DB.getTemplateB(id);

      // Checking if ID was found.              if
((tptRef._tpt == null) || (tptRef._size == 0))
      {
         return ERR_INVALID_ID;
      }
      // Comparing templates.       return
(int)_grfingerx.Verify(ref _tpt._tpt, ref tptRef._tpt,          ref
score, (int)GRConstants.GR_DEFAULT_CONTEXT);
   }

   public int VerifyC(int id, ref int score)
   {
      TTemplate tptRef;

      // Checking if template is valid.
      if (!TemplateIsValid()) return ERR_INVALID_TEMPLATE;

      // Getting template with the supplied ID from database.
tptRef = _DB.getTemplateC(id);

      // Checking if ID was found.              if
((tptRef._tpt == null) || (tptRef._size == 0))
      {
         return ERR_INVALID_ID;
      }
      // Comparing templates.       return
(int)_grfingerx.Verify(ref _tpt._tpt, ref tptRef._tpt,          ref
score, (int)GRConstants.GR_DEFAULT_CONTEXT);
   }

   // Show GrFinger version and type
   public void MessageVersion()
   {
      byte majorVersion = 0, minorVersion = 0;
```

```
      GRConstants result = (GRConstants)_grfingerx.GetGrFingerVersion(ref majorVersion,
ref minorVersion);
      string vStr = "";
      if (result == GRConstants.GRFINGER_FULL)
vStr = "FULL";
      else if (result == GRConstants.GRFINGER_LIGHT)
vStr = "LIGHT";
      MessageBox.Show("The GrFinger DLL version is " +
majorVersion + "." + minorVersion + ". \n" +
         "The license type is '" + vStr + "'.", "GrFinger Version");
   }

   // start enroll
   public int StartEnroll(string _AcctNo, string _CustomerID, string Pin)
   {
      AcctNo = _AcctNo;
      CustomerID = _CustomerID;
      PIN = Pin;
      int ret = _grfingerx.StartEnroll((int)GRConstants.GR_DEFAULT_CONTEXT);
return ret;
   }

   // consolidate template
   public int Consolidate()
   {          int
result;
      int qual;

      // set current buffer size for the extract template
      _consolidatedTpt._size = (int)GRConstants.GR_MAX_SIZE_TEMPLATE;
result = (int)_grfingerx.Enroll(
         ref _raw.img, _raw.width, _raw.height, _raw.Res,
         ref _consolidatedTpt._tpt, ref _consolidatedTpt._size, out qual,
(int)GRConstants.GR_FORMAT_DEFAULT,
         (int)GRConstants.GR_DEFAULT_CONTEXT);
      // if error, set template size to 0
      if (result < 0)
      {
         // Result < 0 => enroll problem
         _consolidatedTpt._size = 0;
      }
      return result;
   }
```

```
   //Importing necessary HDC functions
   [DllImport("user32.dll",    EntryPoint    =    "GetDC")]
public static extern IntPtr GetDC(IntPtr ptr);

   [DllImport("user32.dll", EntryPoint = "ReleaseDC")]     public
static extern IntPtr ReleaseDC(IntPtr hWnd, IntPtr hDc);     //
Database class.     public DBClass _DB;     // The last acquired
image.     public TRawImage _raw;     // Reference to main form
Image.     public PictureBox _pbPic;     // An enrollment process
was started     public bool _isEnrolling;     // Number of
consolidated templates
   public int _numberOfConsolidated;

   // The template extracted from last acquired image.
private TTemplate _tpt;     // The consolidated
template.
   private TTemplate _consolidatedTpt;
// Reference to main form log.     private
ListBox _lbLog;
   //references Main form Auto Extract Check Box
private CheckBox _cbAutoExtract;     //references
Main form Auto Identify Check Box     private
CheckBox _cbAutoIdentify;     //references Main
form enroll button
   Button _btEnroll;
   //references Main form extract button
   Button _btExtract;
   //references Main form identify button
   Button _btIdentify;
   //references Main form verify button
   Button _btVerify;
   // GrFingerX component
   AxGrFingerXLib.AxGrFingerXCtrl _grfingerx;
};
```