Digital Forensic and Biometric Analysis for Information Security and Network Management

By

OHAERI, IFEOMA UGOCHI

(Student Number: 23989688)

A Thesis Submitted in Fulfilment of the Requirements for the award of the Degree of Doctor of Philosophy (PhD) in Computer Science

Department of Computer Science
School of Mathematical and Physical Sciences
Faculty of Agriculture, Science, and Technology
North-West University, Mafikeng Campus

Supervisor: Prof. O.O. Ekabua

Co Supervisor: Prof. M. Esieferienhe

February, 2016

Declaration

I declare that this research on **Digital Forensic and Biometric Analysis for Information Security and Network Management** is my work, and has never been presented for the award of any degree in any university. All the information used has been duly acknowledged both in text and in the references.

Signature _____ Date 19/04/2016

Ohaeri, Ifeoma Ugochi

Approval

Signature _____

Supervisor: **Prof. O. O. Ekabua**
Department of Computer Science
Faculty of Agriculture Science and Technology
North-West University- Mafikeng Campus
South Africa.

Signature _____ 19/04/2016

Co Supervisor: **Prof. M. Esieferienhe**
Department of Computer Science
Faculty of Agriculture Science and Technology
North-West University- Mafikeng Campus
South Africa.

Dedication

This thesis is dedicated to my Mum Hon Chief Mrs Theresa Ohaeri and my beautiful daughters- Flourish Cheryl and Bliss Earlene.

Acknowledgements

Firstly, I wish to express my profound gratitude to God Almighty, for granting me the grace to successfully complete this research work and the programme. To him alone is all the glory!

I am grateful to Prof. O. O. Ekabua, and Prof. M. Esiefarenhe my supervisors for their invaluable support and guidance. Their motivation, advice, useful discussions, useful criticisms and rare patience while carrying out this research work cannot be over emphasized. May the Almighty God bless you two.

I appreciate the North-West University and MASIM for affording me the opportunity and financial assistance to undertake this Doctoral degree. I am also thankful to all the members of staff of the Department of Computer Science, North-West University, Mafikeng Campus, especially, Dr N. Gasela for his support. Without you this work would not have been completed. God bless you.

I express my profound gratitude to Prof Eno Ebenso for his support towards the completion of this research work. God Almighty Bless you.

I further express my appreciation to Dr Bassey Isong, for his valuable contributions towards the success of this research work. God bless you.

I want to also thank my friends and research colleagues, Francis Lugayizi, Thuso Moemi, and most especially Duladi Nosipho and Hope Mogale, for their help and support during the course of this research work.

My unquantifiable appreciation goes to every member of my family for their relentless support in all ramifications throughout the course of this research work, most especially my late Dad, Chief Mojekwu Ohaeri, whose his great love and sacrifices has sustained my dreams to this moment. His self-denials and high aspirations have kept my vision from fading. May his soul rest in perfect peace! I remain absolutely indebted to my Mum, Hon. Chief Mrs Teresa Ohaeri. She has ever been my fountain of inspiration, source of motivation, encouragement and true love; she has never ceased to believe in me. Her immeasurable support kept me going through difficult times. Mum, you remain my hero.

TABLE OF CONTENTS

Chapter 2

Chapter 3

LIST OF FIGURES

LIST OF TABLES

Abstract

The high deployment rate of information systems and networks by governments, colleges, enterprises, individuals, and institutions indicates rapid development of information and communication networks, making effective security mechanisms highly demanded. However, identity convergence introduces additional security and privacy challenges (attacks/threats) which the common conventional and knowledge based security mechanisms such as passwords, PINs, and tokens are inadequate to address. In this work, a review of existing authentication systems design was conducted and the result was the design and implementation of a prototype biometric fingerprint authentication and identification system using North-West University as the implementation domain. Using the prototype, a biometric fingerprint analysis was carried out to determine the uniqueness of each individuals fingerprint using MATLAB. Also conducted was data recovery analysis of an encrypted PDF document using the Advanced PDF Password Recovery forensic tool, the essence of which is to test the viability and usability of the forensic technology. The results from the biometric fingerprint analysis shows that installing fingerprint biometrics authentication as an identification measure provides proper identification and complete information privacy compared to other security platforms. The prototype also enables data in encrypted form to be decrypted for further analysis to be carried out on the data.

List of Acronyms

Acronyms	Meaning
IOCE	International Organization of Computer Evidence
DOS	Disk operating System
SCERS	Seized Computer Evidence Recovery Specialist
ECSAP	Electronic Crime Special Agent Program
CART	Computer Analysis Response Team
CCI	Computer Crime Investigation
DCFL	Defence Computer Forensic Laboratory
FACT	Forensic Association of Computer Technology
FCG	Forensic Computing Group
ACPO	Association of Chief Police Officers
Y2K	Year 2000
G-8	Group 8
SWGDE	Scientific Working Group on Digital Evidence
ASCLD-LAB	American Society of Crime Laboratory Directors Laboratory
FTK	Forensic Tool Kit
ACES	Automated Case Examination System
DCFL	Defence Computer Forensic Laboratory
RCFL	Regional Computer Forensic Laboratory
CART	Computer Analysis Response Team
FEPAC	Forensic Education Program Accreditation Commission
ASTM	American Society of Testing Materials
E-30	A committee
IFIP	International Federation Information Processing Approaches
DNA	Deoxyribonucleic Acid
AFIS	Automatic Fingerprint Identification System
ISSC	Information Security Service Culture

NGI	New Generation Internet
SeCA	Security of Cloud Adoption
TV	Television
CPU	Central Processing Unit
CFIM	Computer Forensic Investigation Model
PKI	Public Key Infrastructure
PD IR	Pro-Discover IR
FTIR	Fourier Transform Infra-Red
DNA	Deoxyribonucleic acid
ACEV	Analysis Comparison Evaluation Verification
IAFIS	Integrated Automated Fingerprint Identification System
ALS	Alternate Light Source
LED	Light Emitting Diodes
LFR	Low False Reject
FRR	False Rejection Rate
FAR	False Acceptance Rate xv
SFinGE	Synthetic Fingerprint Generation
ICC	Intra-class Correlation Coefficient
PDF	Probability Density Function
FA	False Acceptance
FR	False Reject
C1	Category 1
C2	Category 2
N	Number
NWU	North-West University
Uc	Use case
MYSQL	An open source relational database management

PHP	A script language
IB	Information Base

Chapter 1

Introduction and Background

1.1 Introduction

Information Security is a growing and general concern that cuts across all spheres of our society including; business, government, domestic financial, and so on. The information community is highly dependent on a broad range of networks and systems with critical roles which include, among others, public health systems, financial systems, or air traffic control systems.

Information is a critical resource for every institution because of the rapid appropriation of IT (Information Technologies) in their overall business activities. This has increased the need for an effective management of the companies and institutions information. In fact, this has brought about the need for information security and network management. In new generation companies and institutions, this reality is even more pressing because information is one of their core businesses. Thus dependence on Information Systems (IS), and networks has skyrocketed in the last few years, hence there is a need to effectively protect the information that is transmitted across these systems and networks in other to maximize their potentials [1]. Therefore, there is no doubt that today Information Systems and networks play a very important role in society, the economy, and also on critical infrastructures.

Consequently, businesses and organizations, daily, are confronted with huge potential losses due to their heavy dependence on this hardware and software (systems). This has led to the urgent need for Information Security and Network Management (ISNM). The need to be properly secured inside and outside in other to harness their ever increasing dividends is the goal of this research work. We proposed Digital Forensic and Biometric Analysis for Information Security and Network Management. This is due to the current increase in using Information Systems and networks which are found clustered all over the internet. This has led to a lot of new security attack threats [2].

However, this indicates that the current-day Networks and Information Systems distributed across the internet are quite vulnerable to huge threats and attacks which include; social engineering attacks (phishing), cyber-attacks from cyber terrorist, and hackers, including inappropriate use of the network access by the authorized users. The tremendous growth of security in computing indicated in 2009 by ITU has led to the design and implementation of a

large number of techniques, frameworks, models, and protocols by many researchers which are regularly updated by more researchers building on the platform.

However, innovations are proposed on a frequent basis as the need for information security and network management cannot be over emphasized. Apparently, the increasing complexity of Information Technology (IT) infrastructure and security threats which are constant and universal in nature have compelled organizations and institutions all over the globe to review their approaches towards information security and network management. Suddenly, the necessity to increase internal security measures by demonstrating and maintaining adequate security management processes have become the concern of most organizations. Therefore, combating the emerging threats and attackers in today's dynamic Information Communication Technology (ICT) environment requires a more effective security infrastructure designed and integrated using biometrics features. This will enable digital forensic investigations and findings to be developed. Biometric features guarantee easy identification of systems and network hackers, and if they are identified they can then be presented in court for prosecution. This will help reduce the rate at which crime and attacks occur. Therefore, this research proposes Digital Forensic and Biometric Analysis for Information Security and Network Management. This will lead to a significant step in tackling information security and network management challenges [3].

The term security and information systems are closely inked, and it indicates that the security of any organization or institution is as good as the security mechanism deployed. A secure information system is an indication of certainty that aids in creating value both inside and outside the organization.

The mission of Information System Security is to develop security policies with their related measures or processes and dominance components over their information assets. The main goal is to guarantee their integrity, confidentiality, authenticity and availability. To ensure these four goals of security is to ensure the core objectives of Information Security and Network Management.

Organizations are becoming alert to the need of having efficient Information Systems with proper management. Thus, there cannot be any useful information systems and networks without adequate security management systems and the associated security measure. Therefore, it is very important for organizations and companies to adopt security measures that will help them stabilise their systems or networks as well as detect and handle any risk or

attack they may be subjected to. However, implementing these controls is not enough, institutions and organizations should learn to manage information systems and networks over time so as to enable them to respond to current threats, risks as well as vulnerabilities in a spontaneous manner [4,5, 6].

Information security and network management entails trust. It is very important that companies and institutions ensure that they maintain privacy when obtaining and dealing with users' personal information or personal identifiable information (PII) [7]. In today's information society privacy is a prime concern. Privacy focuses mainly on control mechanisms relating to information security. Therefore, there cannot be an efficient and effective privacy mechanism without a strong information security platform. Systems and network users want to be assured that their identification profile and personal details remain private. Therefore, the challenge now is to effectively develop computing systems with privacy protection mechanisms [8]. This is why we proposed Digital Forensic and Biometric Analysis for Information Security and Network Management

However, one of the widely accepted principles of management is that if an activity cannot be measured, it cannot also be managed and analysed. Therefore, metrics can be used as an effective tool for information security management (managers) to check the effectiveness of different security mechanisms to confirm if they are administering the maximum security that is required of them. Many of the various security mechanisms in use today are not very efficient in ensuring that a system or network user is who he or she claims to be and is an authorized user of the facility it requests and yet they are being deployed. Though one hundred per cent (100%) security can never be achieved because of the nature of systems and network vulnerability identification tools available, improvement on current mechanisms is one of the goals of security. For this reason, we propose digital forensic and biometric analysis for Information System and network management. Also Metrics can be used to identify the level of risk associated with not deploying an effective security mechanism. This research tends to point out aspects of password authentication and identification which do not guarantee accurate user identification, and do not also enable digital forensic investigation.

Digital forensic and biometrics are tightly coupled. Forensic information can be available from biometric systems. This means that biometric authentication system precedes digital forensic but they are integrated by analysis. Therefore, this research intends to establish a link between digital forensic (DF) and biometric technology (BT). Also, establish a possibility of

biometric based authentication enabling digital forensic investigation. It is well established that biometric features provide a better access control, identification and authentication of any given party which helps in forensic investigation and digital evidence discovery (Source of this information as Name, Date). Digital forensic investigation involves a group of defined procedures and tasks for experimental purposes. These procedures and tasks are used to extract useful information from digital evidences to commence legal proceedings in court.

However, the procedures includes: preparation, data collection, examination, data analysis, and reporting or presentation of findings. Preparation and data collection is the initial phase of the process which basically identifies, labels, records, and acquires data that are relevant data from every possible sources of information that are available. The second phase is examination which involves the forensic processing of all relevant data that are collected either by automated or manual means or a combination of both to extract and obtain particular data of interest. The next phase in the process is the analysis of the results obtained from the examination phase. This entails obtaining helpful information that discussing the questions that comprises the aim of performing data collection and examination using procedures and techniques which are legally accepted and widely justifiable. The last is reporting which entails the ability to communicate the results or findings obtained from the previous phases of the process which includes the detailed description of the actions performed, the explanation of the tools and procedures used and how they were being selected. If there is a need, other actions that should be performed may also be included. In addition, recommendations on how the procedures, policies, controls, tools and guidelines utilized in the process can be improved and other areas of forensic process may be included [7,8,9].

However, analysis is one of the core and complex stages of digital forensic process. It is the main aspect of this research work. The analysis stage of forensic investigation involves; data analysis, survey, extraction and examination. Digital forensics as defined by the digital forensic research workshop (DFRWS) is "the use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purposes of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations". This definition embraces the wide aspects of digital forensics beginning from the acquisition data to the stage of legal actions. Analysis begins after data has been acquired or

collected from the suspect system or crime scene. It basically involves critical extermination of the acquired data in order to identify evidence. Therefore, digital forensic analysis can be referred to as identifying digital evidence which are scientifically obtained using proven procedures that can be used in facilitating or reconstructing of events during an investigation period [10,11, 12].

Obviously, like any other investigation of events, to find the truth data must be identified in order to either verify existing data and theories or to contradict existing data and theories. Before both evidences can be extracted from collected data, it must be thoroughly analysed and identified. The task or challenge of digital forensic analysis is to identify the necessary evidence for legal proceedings in court [7, 8, 9]. On the other side, biometric identity-based verification and authentication technology offers more reliable individual identification which supports digital forensic investigation. One of the questions this study will address is: can we analyse, design and implement BT using a fingerprint biometric-based authentication system to enable digital forensic perspective? It presents a prototype biometric fingerprint authentication system while justifying the corresponding research objectives providing answers to the corresponding research questions.

Biometric systems are directly connected to a person because they make use of an individual's unique feature for identification and authentication. Even if biometric data of someone is altered or deleted, the main source of the data from which it was expected remains intact, and can neither be altered nor deleted. Biometric technology which includes Figure 1.2, and Figure 1.3, has been welcomed globally due to its potentially easy authentication, and unique identification.

Figure 1.1: Digital Devices

Figure 1.2: Fingerprint Biometric. [8]

Figure 1.3: Face Biometric [8]

The use of finger print readers and face recognition biometric systems is very convenient. Apparently, there are no two persons in the world with the same face and same finger print. It is not possible for a person to deny the use of face and finger prints because there is no proof that someone else used your face or went out with your hands when you have them with you. Biometric data are efficient access control measures and they are a key element in digital forensic analysis. The data help to boost the level of security in information systems and networks. Also, it makes identification and authentication procedures more robust, fast, effective and convenient [10, 11, 12].

The positioning of face recognition devices and finger print readers as access control measures will help to solve the problem of individual untraced movement within a system and network. More so, it will contribute to a drastic reduction of cybercrime and network attacks making security systems more reliable. Consequently, faces and finger prints can totally replace the numerous cards, codes, signature, and passwords which people carry around. Therefore, one of the efforts of this research study is to support the development and advancement of digital forensic and biometric technology such that the capability of digital forensics in identifying biometric features involved in incidents is upheld to enhance information systems and network security and provide better quality of network management service.

However, in forensic perspectives, it is quite possible to extract more information from biometric access devices. The images in Figure 1.4 show devices with fingerprint authentication mediums.

The small rectangle mounted at the bottom right of the keyboard is the fingerprint sensor. The measure will discover increasing applications in securing laptops.

Storing the biometric information in a standardized manner in the database makes it possible to locate statistical data and also have more information regarding the peculiarity of the biometric feature. However, every biometric system must consider the intrusiveness of data collection and other factors which include; throughput rate, requirements for data storage, enrolment time accuracy, and acceptability to users, speed, uniqueness, ability to resist counterfeiting, and reliability must be justified in order to be effective. Adopting and implementing this system at borders, banks, pay points, entry to facilities, and others, definitely makes identification more reliable due to the extra information about every individual at every location which is readily available. Therefore, if biometric systems can be adopted and properly implemented by every institution, they will culminate in a more reliable identification measure which in turn aids forensic processes and associated legal actions [10, 11, 12].

1.2 Background Information

The term security and information systems are closely linked, and it indicates that the security of any organization or institution is as good as the security mechanism deployed. A secured information system and network is an indication of trust that helps in building value both inside and outside any institution.

Information Systems and Network Communications have become part of everyday life. In recent times, there has been a massive growth in computer and electronic devices as well as systems that are network-based either for e-government, e-commerce, or internal processes inside institutions or organizations. Human beings can no longer be separated from electronic devices and the internet technology. The need for information security is increasing rapidly as a result of the quantity of information that is made available on the systems and networks that are interconnected on the internet [13]. Meanwhile, a concurrent increase has been recorded in the rate of cyber-crime; a rise in information warfare, and threats of cyber terrorism. As a result of this huge increase many organizations, companies, and even nations now thoroughly

scrutinize the security of their critical infrastructures for information systems, and network - based attacks. This is due to a high rate of reliance on information systems and networks including the data that is processed, transmitted and stored by them.

Therefore, it is critical to provide an effective security measure and system that ensures the integrity, confidentiality and availability of the information systems and networks, including the services and resources which they provide. This can be achieved using digital forensic and biometric technology (DFBT). The invention of the field of computer forensic science was to provide a means of suppressing computer and network attacks which was on the increase [14]. Digital forensics was to provide a proven and justified process of investigating computers and other digital devices which are suspected of being involved in any form of criminal activity and network attacks [15]. Proper digital forensic procedures and process models should be followed for its evidences to be acceptable in any court of law. Digital forensics applications cover several aspects which includes the need for the law enforcement agencies to produce compelling and legally acceptable evidence required to prosecute an offender, (the need for institutions and cooperation to identify and mitigate insider threats [16]. Tools for computer forensics are used in collecting, analysing and extracting evidence from computers and networks after intrusions are made on private or confidential information [17, 18, 19, 20]. The demands for investigation forensic tools and procedures have already outweighed current capacity. Therefore, this research proposes digital forensic and biometric analysis for information security and network management. It aims at establishing that biometric feature authentication guarantees accurate user identification, and also enables digital forensic investigation should there be any security violation and attack. It provides legal evidences which are admissible in court for prosecution of offenders and attackers. However, it is evident that the growth in electronic transactions increases alongside with malicious activities and network attacks. The rate of computer crime is steadily increasing, attackers and intruders are at liberty to exploit systems, and disrupt networks without the risk of suffering the consequences. However, combatting these attacks has become a major global concern [21].

Apparently, information security and network operations encompass a lot of disciplines which can be applicable in military, political, and corporate spheres with the goal of gaining a competitive advantage. The International Standard Organization (ISO 17799) has defined information as "an asset that may exist in many forms and has value to an organization, industry or institution".

Therefore, the objective of information security is to efficiently and effectively secure this valuable asset so as to minimize business damage, guarantee business continuity, as well as maximize investments returns. In addition, information security is characterized by the preservation of integrity methods, confidentiality, and availability according to ISO 17799. Needs for information systems security and trust vary depending on the system and or network but, the basic requirements include: confidentiality, integrity, and availability [22].

I. Confidentiality

This requirement of information system security ensures privacy and protection of data stored in a system or during transmission. It controls unauthorized profiling of users IDs. It ensures that sensitive information is not disclosed to unauthorized recipient, except the parties involved in the communication.

II. Integrity

This requirement ensures that programs and information are altered, modified or changed, in a required and authorized way. All modifications of information, data or programs are made by the explicit consent and authorization of the parties involved. This entails that data can only be changed by the authorized entities in authorized manners or for personal advantage.

III. Availability

This requirement assures that authorized entities can access all the information and resources provided continually, and timely. It guarantees the proper functioning of all systems such that there is no denial of service to all authorized users. All assets are available and accessible to all authorized users at appropriate times. It ensures that attackers are stopped from flooding a network with huge traffic that delays authorized traffic that containing new commands from being transmitted [23].

In addition, the accountability requirement cuts across these previous three requirements. It involves knowing who has accessed available information or resources. It is evident from the list that security entails more than ensuring that information is not disclosed. Therefore, in order to justify these security requirements certain security services such as authorization, authentication, auditing, and non-repudiation are also required.

A. Authentication

This is an access control measure that establishes that a message is from the source it claimed to be from and the party is indeed who he or she claimed to be. Generally it verifies both the identity and the authority of a party and prevents unauthorized access to information, system and networks. This is usually in the form of a password, a hardware computer-readable token, or a fingerprint.

B. Authorization

This is a security measure that checks if a user is permitted to access the network services or perform certain tasks. This process grants a party the right of access and the privileges to perform a specific action or group of actions.

C. Auditing

This activity records the operations that are invoked alongside the identity of the entity that is performing it including the object that is acted upon and also the later examination of these records.

D. Non-repudiation

This involves using digital signature procedure to consolidate the integrity of a specific message and the identity of the creator in protecting against any attempt to deny authenticity of the message [24, 25].

Consequently, information security can be explained as processes, and techniques that limit information access to only authorized clients, protects information against unauthorized alteration, and ensures the accessibility and availability of information whenever needed. This definition holds for both the information transmitted or stored on computers, stored on printed media, computer storage media or in network services [26]. In addition, Information Security and Network Management (ISNM) consists of administration and control development, provisioning functions and maintenance of operations required to monitor, provide, interpret, as well as control network and the services it provides. When data has been processed and it is usefully utilised, it is regarded as information. A user's raw details are referred to as data, and when it is processed for useful purposes it is referred to as information [27]. Systems are computers and electronic devices that are designed for communication. All together they form a network when they are interconnected locally or globally to enable a wider coverage and dissemination of information [28]. Information systems and network

security starts at the top and it is everyone's concern. Oftentimes, security is based on rarity of design and implementation of systems and networks. This results in systems and networks breakdown within a short time.

Hence, security should be felt at all levels of systems and networks design and implementation for maximum productivity [29]. Attacks are easier, faster, and cheaper than protection and security. In fact, there are more experts in attacks than there are in protection and security because of its rewards [30]. Developers are busy designing tools for systems and networks attacks; there are so many workshops on the use of sophisticated tools to discover systems and network vulnerabilities for exploitation [31]. For this reason, the essence of security should not be under-emphasized. It is important to adopt access control mechanisms that enhance an organization's capacity to control access to information (assets) based on various requirements. These requirements can include security requirements and business requirements. Business requirements consist of various policies and access control mechanisms such as policies and procedures that control access to organizations assets on the basis of the host and clients management requirements. Host and user management consists of measures to register and deregister users; review and control of assets and privileges, authentication and authorization profiles management. System and network requirements consist of mechanisms for most system access control and network access control and host access control, including application access control.

I. *System and Network access control:* This control allows policies that monitor the usage of systems and network services. Whenever required the mechanism must authenticate nodes, authenticate nodes and external users, define protocols and routing, control both network and device security, as well as maintain network segments and connections, and also maintains the security of network resources and services provided.

II. *Host access control:* Whenever it is appropriate this control automatically sets up measures that identifies terminals, and authenticates users, manage security profiles, secure log-on, secure system utilities and enable terminal, as well as, connection or user timeouts.

III. *Application access control:* Within this control, access to application is limited basically by the user or application authorization levels. Access monitoring measures and monitors system access and use in other to identify unauthorized activities.

More so, mobile computing policy, principles, and standards handle asset protection, secure user responsibilities, secures user access, and user control [32, 10, 33]. Therefore, there is a need for improvement on the present security methods and discoveries to implement the defined policies such that intruders and attackers can easily be identified and prosecuted. Moreover, as people and devices get interconnected globally there is a need for reliable user authentication mechanisms to establish that a person is who he or she claims to be [21]. Therefore, determining identities to ensure that only authorized users of a specified facility are given access becomes a crucial issue. Also, supporting the law enforcement agencies with computer-based evidences that determines who, what, where, when and also how for appropriate representation of computer and digital crimes [34, 35].

Obviously, a reliable user authentication mechanism is required to provide valid user identification because, until a suspect is proven guilty, he or she cannot be convicted. It is important to ensure that people do not commit crimes without getting the due penalties. Hence, security forms a vital aspect of information systems and networks. It is to be given the upmost priority in every system and network development cycle to ensure stability, productivity and quality of service (QoS). Thus, Digital Forensics and Biometric Analysis for information systems and network management can be utilised for stronger information security and network management [36, 37].

This study centred mainly on how to better identify users or parties to enable forensic investigations such that culprits (attackers and intruders) are identified and prosecuted. This study therefore, proposed Digital Forensics and Biometric Analysis (DFBA) for Information Security and Network Management. It specifies the significance of biometric features such as fingerprints in forensic analysis. Also, it emphasizes that the use of biometric authentication will enable forensic findings and investigations [38].

Information security is part of the overall network management principles required in order to prevent the wrongful use, loss or improper access, alteration or disclosure of personal information or details, prompt identification of breaches of privacy, and also timely and proper response to potential privacy breaches in a timely and appropriate manner. Information security and network security technologies protect systems and networks against theft and all forms of misuse of confidential business information, internet worms and

viruses, all forms of system and network violations, unauthorized intrusions, service and network disruption and enables legal action.

However, in this study, DFBA is basically proposed to mitigate attacks and systems violation by identifying not only the attack but also who the offender is to support legal proceedings. In so doing, attacks are no longer rewarded but penalised [38]. Therefore, Digital forensic (DF) is referred to as a process of establishing and relating extracted information and relevant digital evidence in order to determine useful information for legal review, and biometric data is based on physical or behavioural uniqueness of a person [39]. Implementing unique policies can prevent unwanted access to the network or system via automated biometric control methods. This verifies special physiological features or behavioural characteristics in order to identify an individual. Analysis collects all data, evidences and findings to obtain an overview at a crime scene for the purposes of identifying and clarifying information gathered through the previous stages of investigation for further investigations and legal proceedings. Through analysis, there is justification that all data was captured accurately and common trends and patterns were identified. Apparently, this research intends to take security another step further to identify attackers and not just ward them off via access forbidden automated responses. This will help to reduce the high rate of attack and attack experts that are steadily on the increase [40, 41].

The classical biometric systems that focused on face recognition and fingerprint technology have been known for a long time. They are used for two different main tasks such as; access control and forensic investigation. We can refer to them as joint systems. In the description of the main concept of the Biometric Security System, the biometric features (data) must not only serve as access verification or identification, but can also be used for data protection to enable forensic investigations. We can ask the question, 'Is it possible to generate some of the biometric features such as face and fingerprint or thumbprint for better forensic findings?' There is enough information entropy in the fingerprint to generate suitable digital evidences [39]. Therefore, we introduced the combination of Digital Forensics and Biometric Analysis as a more reliable security mechanism, using a thumbprint or fingerprint as a corresponding feature for identification, and extraction of digital evidence for legal proceedings [42]. Hence, analysis of biometric devices can be imperative since additional information of every individual who wants to access a facility or a computer system or network is usually made available. In hacking cases this measure can be useful if the suspect logged using biometric data such as a face or a fingerprint [30, 43, 44].

Network forensic systems are concerned with capturing, recording, and the analysis of network traffic for detecting intrusions and investigating them [45]. Digital Forensics interprets and preserves all digital evidences in its most original form while proceeding further investigations, while, biometric systems address pattern recognition with operations that acquires biometric profiles from a person, extracts a feature set from the acquired data, and compares the sample against an initial registered template [46]. The application determines if the template can be stored in the system's/network's database or in a token, such as smart cards. Biometric techniques describe these unique distinct biological characteristics that identify a person and differentiate one from another. These biological or behavioural characteristics can be used for automated recognition [47]. Biometric data verifies and confirms an individual's claimed identity by comparing the current submitted image with the previously captured image. The verification application includes both physical and logical access control while forensics is concerned with gathering and analysing of physical evidence from a crime scene to identify the culprits. Biometrics is a reliable access control and authentication mechanism that can be applied in digital forensic [48]. Developments in ICT have increased performance and provisioning of equipment at a lower cost which has created a route for automated biometric recognition systems. Biometric applications can be categorized into three main sets such as Government application, Commercial applications, and Forensic applications.

I. *Government applications:* This category can be used in personal identification documents, such as ID cards, passports, driver's licenses, border or immigration control; welfare-disbursement, social security cards; voter registration and control during elections; and others.

I. *Commercial applications:* This category can be applied for physical access control; logins to network and systems; e-Commerce, and ATMs; credit cards, and device access to computers; mobile phones, and PDAs; facial recognition software, and e-Health, and others [47].

II. *Forensic applications:* This category can be used for criminal investigations, in identification of corpse identification, in determination of parenthood, in break-ins into buildings, cars, and others

Apparently, Biometric and Forensic data can operate together to analyse human features at crime scenes for proper identification of the culprits and their victims. Digital forensics and biometrics over-lap and support each other at crime scenes to gather useful and positive

identification for legal proceedings [48]. Therefore, we intend to focus our analysis on physical access control and forensic application categories.

From forensic perspectives, even more information can be extracted from the biometric access devices. The images in figure 1.4 show some electronic devices with fingerprint authentication medium. The measure will find increasing application in securing laptops.

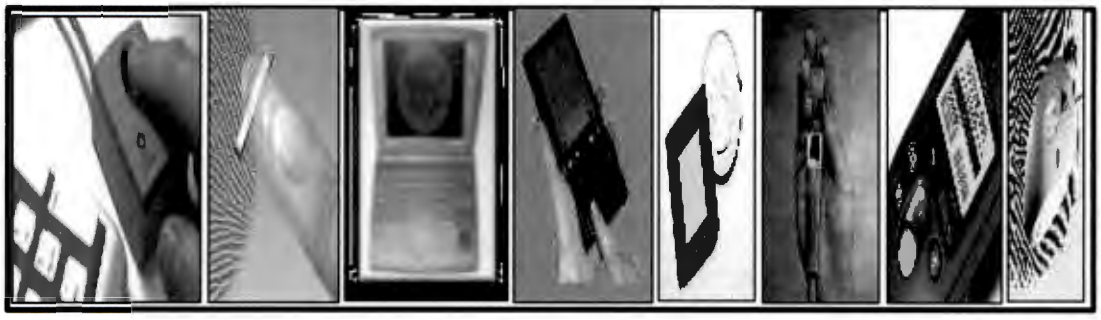

Figure 1.4: Devices with Fingerprint Authentication Features [11]

Hence, we shall report this study on digital forensic and biometric analysis for information security and network management in two sections namely; Biometric Analysis and Digital Forensic Analysis. Biometric Analysis took precedence in the actual presentation in the thesis as opposed to the appearance in the thesis title because we did the study from the application domain point of view. In that sense, we first discussed the biometric template generation, the biometric system design, and later the digital forensic technology as a measure to identify impostors, intrusions and offenders in cases of incidents. This we described clearly in the research questions and the corresponding research objectives.

1.3 Statement of Problem

The invention of the conventional security mechanisms such as user names and password – based authentication emerged as a solution to mitigate unauthorized access to information/data, systems, and networks in order to ensure adequate privacy and protection. This created some level of confidence to electronic systems and device users, but the questions are: can this security mechanism be trusted? Is it totally reliable? Of course, the answer is no. Over the years it has been discovered and acknowledged that password–based authentication mechanisms can no longer guarantee maximum security of information, systems and networks due to the level of risk associated with it [49]

Consequently, passwords are likened to "low-hanging fruits" due to the manner in which users choose passwords. Often users either choose easy-to-remember PINs or passwords and most times they write them down for fear of forgetting them. This makes the passwords and PINs vulnerable to socially engineered attacks such as password sniffing, cracking and capturing [50]. Sometimes the passwords are even completely forgotten, making the services inaccessible at urgent times. The interfaces between the information, systems, networks, and the users are regularly abused, as people are subjected to remembering many complex passwords and carry tokens within their various daily activities. However, this makes it difficult to ensure the integrity of the processes. Confidentiality and availability of data in any communication are the core fundamental requirements of any effective security mechanism [29]. More so; attackers commit crimes with ease without the fear of being caught because their actions are untraceable. These challenges have heightened the need to provide better individual identification and a more reliable user authentication mechanism to establish that a person is who he or she claims to be and he or she is an authorized user of a facility, information, system, or network. Therefore, this research investigates the use of Digital Forensics and Biometric Analysis for Information Systems and Network Management in order to create a reliable and secure communication domain. Digital Forensics extracts digital evidences by investigating from digital information, produced, stored, or transmitted by computers or electronic devices for legal proceedings. The use of biometric authentication will enable digital evidence discovery during a specified investigation procedure because it is easier to identify people by their features than with passwords and PINs [51].

1.4 Research Questions

In consideration of the above stated problem, this research would be addressing the following research questions (RQs):

RQ1: Can we analyse and implement Digital Forensic Technology to support Information Security and Network Management?

RQ2: Can we analyse and implement Biometric Technology to support Information Security and Network Management?

RQ3: How can fingerprint minutia point extraction and matching be performed to support Information Security and Network Management?

1.5 Rationale of Study

The need for security is presently a global concern. This is because of the huge dependence on systems and networks for effective operation at all levels.

Therefore, the analysis in this research shall be conducted in two sections. Digital Forensic Analysis takes the first section while Biometric Analysis will take the second section, as indicated in the Title.

Biometric Analysis is conducted based on the five basic components (modules) of fingerprint authentication and identification system which includes Enrolment/Sensor Module, Minutiae Extraction Module, Database Module, Matching Module and Decision Making Module [44, 52, 53].

A. *Enrolment/Sensor Module:* This module captures the biometric features of an individual via the sensor or scanner device. The expressions of the captured feature are submitted for minutia extraction. An example is fingerprint sensor or scanner that captures fingerprint impressions of users.

B. *Minutiae Extraction Module:* In this module the region of interest is extracted from the acquired feature. In a fingerprint image, the orientation and position of minutiae points are extracted in the feature extraction segment of the system.

C. *Database Module:* A database module or component is designed to store or hold the information which is used in matching new captured templates for resemblance.

D. *Matching/Comparison Module:* In this module the feature minutiae points are matched against the templates for resemblance and identification. This is determined using the obtained matching score.

E. *Decision Making:* In this module, the users claimed identity feature is determined to be either rejected or accepted depending on the matching score.

While the digital forensic analysis phase of this study is based on the main stages of the digital forensic process model which include Obtaining and imaging forensic data; Obtaining Forensic request; Preparation, and Extraction; Examination, and Analysis; and Forensic Reporting and Case Level Analysis phases [54, 55].

i. *Obtaining and Imaging Forensic Data stage.* This phase of the process recognizing incidents via indicators and determines the type. It is not strictly within the forensic field rather it is embraced as a result of its impact and support to other stages. In some digital forensic, processes and model, are not included.

ii. *Obtaining Forensic Request stage.* This stage of the process utilizes certain procedures that exist which should be followed in securing the right from the relevant bodies to commence the digital forensic process.

iii. *Preparation and Extraction stage:* of isolates, secures, and also preserves the state of both physical and digital evidence at a crime scene. It ensures that digital or electronic devices connected to affected devices or network or areas are prevented from further usage. On the other hand it involves identifying, isolating, labelling, recording and collection of data and other physical evidence relating to the incidents being investigated, as it establishes, and maintains the integrity of the evidences via a chain of custody.

iv. *Examination and Analysis stage:* In this phase the examination phase of the process identifies and extracts relevant information from the collected data via proper forensic tools, techniques, and measures, while it continues to maintain integrity of the evidences, while, the analysis stage of the process analyses useful/appropriate answers to questions that were presented from the previous stage of the forensic process. This is the main focus of this research study.

v. *Reporting and Case Level Analysis stage:* This stage of the process involves proper presentation of the results obtained from the previous stage that leads to a conclusion on a suspect. This stage consists of the following: relevant information relating to the case: action performed; action yet to be performed; and recommendations for improvements on procedures and tools that are recommended. And the case level analysis is the process of identifying any problem that needs immediate attention during reporting.

1.6 Research Goal and Objectives

The goal and objective of this research study were:

1.6.1 Research Goal

The goal of this research was to analyse Digital Forensics and Biometric Technology for Information Security and Network Management.

1.6.2 Research Objectives

To achieve the goal of this research, we had the following objectives:

1. To analyse Digital Forensic Technology using a Digital Forensic process model to support Information Security and Network Management.
2. To analyse BT using a fingerprint-based authentication system to foster a reliable identity management system.
3. To analyse fingerprint minutia point extraction and matching in a biometric-based authentication system to enhance Information Security and Network Management.

1.7 Research Methodology

The methodology to be used in this research consisted of three steps, which were: literature survey, DBFA analysis, prototype implementation as a proof of concept, and result analysis.

Below is the research method in detail:

1.7.1 Literature Survey

This method will involve the survey of existing research materials that have been done on biometrics and digital forensic analysis for information security and network management.

1.7.2 Design Approach

Based on the knowledge and the information obtained from the literature reviews and component description, the analysis of the biometrics and digital forensic technology was presented using (1) biometrics and digital forensic architecture, (2) fingerprint authentication and identification system flowchart, and (3) Digital forensic process model.

1.7.2.1 BDF Architecture Design

With architectural design, the different processes involved in biometric and digital forensic analysis were presented in this thesis. The BDFA is an integrated design of a biometric and digital forensic technology that depicts how fingerprint biometric system compliments digital forensic science.

1.7.2.2 Flowchart Design

The flowchart designed in this thesis is the fingerprint authentication/identification system flowchart. It consisted of two main components: the enrolment of the user fingerprint into the database using a fingerprint sensor/scanner, and the authentication and identification of the user using the captured fingerprint sample.

1.7.2.3 Model Design

The model that designed in this thesis was based on existing models. It was used as a guide to design a standard to analyse the stages in digital forensic process.

1.7.3 Proof of Concept Approach

The proof of the concept methodology was employed in order to validate the research ideas. This method consisted of a detailed analysis of a biometric authentication and digital forensic process to enhance information security and network management.

As proof of concept for this thesis, we reported:

I. Analysis of digital forensic technology to foster information security and network management with emphasis on impacts and challenges.
II. Analysis of biometric technology to enhance Information Security and Network Management.
III. Analysis of the requirements for developing the fingerprint biometric authentication system that provided effective information security and adequate network management was carried out.
IV. A prototype fingerprint biometric authentication system designed and implemented with emphasis on attendance and access control.

1.8 Research Contribution

The main contribution of this thesis to the research community, academia, and information and network security experts is the development and implementation of digital forensic analysis process model and the biometric authentication/identification system flowchart. This thesis presents a methodology for conducting digital forensic and biometric analysis in order to address the insecurity issues working against information and networks management systems on a daily basis. Categorically, the digital forensic and biometric analysis discussed

in this thesis contributes immensely to the research community, academia, and information and network security experts in several ways which includes: Fostering the need for adopting biometric authentication as that can enhance digital forensic investigations in cases of crimes involving identification this we achieved by developing a biometric attendance system; Supporting the essence of digital forensic investigation as a reliable measure in identifying cybercrimes and their perpetrators this we achieved by implementing the Advanced PDF Password Recovery Window; and Promoting the reliability of fingerprint minutia matching, this we achieved using False Acceptance Rate (FAR) and False Rejection Rate (FRR) metrics.

1.9 Included and Related Publications

This research study builds on some previous studies which have been published in conference proceedings and journals. In this segment, we present extracts of the thesis that have been published while some are still under review. The manuscripts include:

i. **I.U. Ohaeri,** O. Ekabua. **"Generic Architecture for Biometric and Digital Forensic Analysis"** published in the International journal of Soft Computing and Engineering, Jan. 2015.

ii. **I.U. Ohaeri,** M. Eserferienh, N. Gasela, **"Multimodal Biometrics as Attack Measures in Biometric Systems"** published in the proceedings of International Conference on Wireless Networks, ICW 2015, Las Vegas, Nevada, USA, July, 2015.

1.10 Thesis Structure

The structure of this thesis includes:

Chapter 2 gives a comprehensive literature review of the existing research work on biometric and digital forensic technology and their overview in accordance with the objectives of the thesis. The key terminologies used in this research study are also explained.

Chapter 3 provides the digital forensic analysis model as a platform to conduct the analysis of digital forensic technology. The components of the DF model were discussed extensively and methodically. Some of the stages of digital forensic analysis technology were applied in order to implement the widely accepted security mechanism

Chapter 4 discusses the biometric concepts in the analysis perspective. It reports the Analysis of Fingerprint Minutiae Point Extraction. It detailed the stages involved in generating and extracting the fingerprint minutiae point in order to determine the uniqueness of a fingerprint which guarantees the security of information systems and improves network management.

Chapter 5 describes the analysis of fingerprint biometric minutiae point matching which is basically the stage where identification is determined after the analysis of minutiae extraction point has been successfully analysed.

Chapter 6 provides the practical aspects of biometric technology. The chapter consists of the requirement analysis, implementation and result analysis of the prototype biometric fingerprint authentication and identification system that enhances information security and network management.

Chapter 7 is the concluding chapter of this thesis. The chapter starts with summary, followed by conclusion and recommendations and finally, the research limitations and suggestions for future work.

Chapter 2

Literature Review

2.1 Chapter Overview

This chapter provides the literature on digital forensic and biometric technology in order to draw attention to the significance of the research work. Forensic science tends to apply the wide range of science to areas of interest in judicial system which relate to cases of civil action and criminality. It is pertinent in the easy processing of the criminal justice system specifically in terrorism combating crime.

2.2 Key Terminologies

This section of research provides the definitions and explanations of some the concepts, and key terminologies that are used frequently in course of this research. Moreover, the definitions and explanations are within the context of the research idea. The concepts includes: Security, Digital Forensic and Biometric Analysis, Information Systems and Networks, Cyber-attacks and attackers, Authentication, identification, Verification and Validation, and Authorization.

a. Security: Security is a system that has a main goal of providing control of access within a system or network to ensure a secured communication in order to guarantee quality of service and maximum productivity. It forms a vital aspect of information systems and network. This research focuses majorly on information systems and network security. The explosive advancement in computing power has made possible interconnection of computers and devices around the world including sharing of information. The increased innovation in the use of information systems and networks have raised the value of information and is equivalent to money, thus increasing the risks associated with it as well as the concern of security and protection. The cyber space has become a potential place for attacks and crime. If information is money then companies and different institutions should be held responsible for their security. This research emphasizes that access to information and networks should be monitored and controlled using stronger authentication mechanism such as biometric technology which supports digital forensic investigation in cases of crimes and attacks. Security guarantees quality of service. Therefore, any system or network without security cannot remain relevant.

b. Digital Forensic and Biometric Analysis: Digital Forensic Analysis links persons, places, and things to previous incidents, while Biometric Analysis measures personal behavioural traits and physical attributes which are used to validate the identity, or to verify the claimed identity, of an individual via an automated process. Analysis collects series of information or facts that will be of value in investigations of crimes and relates them to the previous information documented earlier about the operational environment and reviewed based on previous incidents pertaining to a suspect. Apparently, analysis gives rise to new set of facts until the right offender or impostor is identified. This forms the basic idea of this research project.

c. Information, Systems, and Networks: Unprocessed information is raw data and on its own has relatively limited utility. Data collected via a sensor and processed into a useful form becomes information and virtually obtains higher value and utility. However, the operational environment for the processing and dissemination of information is referred to as a system, whereas, its interconnections for sharing and communication is referred to as a network.

d. Attacks and Attackers: System and network violations or disruptions are referred to as attacks. Attacks occur when an unauthorized party or an intruder attempts to gain entry into the system or network to disrupt the flow of information with a harmful motive. Attackers or intruders are those malicious users who attempts to breech or violate system or networks security interfering with system or network availability, or data confidentiality, and data integrity.

e. Authentication: This is a network security measure that is able to reliably verify and validates a user's claimed identity. It is a fundamental component in human interaction with systems. Traditional measures of authentication that are basically codes, PIN numbers and passwords have dominated computing until recently when a stronger authentication technology such as biometrics started creating awareness of its potentials. It is capable of providing a stronger degree of certainty that a user is really who he claims to be, or is not really who he claims to be. Biometrics is required for a more reliable authentication. This will go a long way in enabling forensic technology identify who exactly a culprit is, and present accurate evidences to commence legal actions. By this, the rate of cyber-crime and network attacks will reduce.

f. Identification: This means finding out who an individual is or recognizing an individual based on a particular feature.

g. Verification and Validation of User Identity: Verification and validation is a process of checking and determining if the user requesting for access to the network service is who he claims to be and, that is, if the login identification details (username and password) supplied corresponds with the identification information already stored in the database to establish access to the network for legitimate users of the network and restrict access to malicious intruders into the available network service.

h. Authorization: This is a security measure that checks if a user is permitted to access the network services or perform certain tasks. This decision to either grant or deny access takes place after the authentication process.

i. Access Control: Access control is a security capability for monitoring and controlling access to the information made available in a system or network. It is mainly to ensure information security and adequate network management.

However, often times verification, authentication and identification are used interchangeably. This occurs most especially when both terms can be attributed to the context or subject under study. In this work we did use them interchangeable due to the context or subject of the work

2.3 Development and Advancement of DFBT

In this section we explain how digital forensics and biometric technology came about. The explanation incorporates their development which involves the history of DFBT.

2.3.1 Developments in Digital Forensic

Computer forensics in practice involved the collection, analysis and reporting of digital data in such a manner that supports legal actions. Digital (computer) forensics is defined as the "analytical and investigative methods that are used in preserving, identifying, extracting documenting, analysing and interpretation of computer media or digital data that is encoded or stored for the root cause or evidence analysis". In addition, the process of acquisition and analysis of digital evidence; identification of sources and suspects; authentication of documents; and order are also involved in digital forensic processing. The acquisition and analysis of digital evidence is a forensic science process that consists of the recovery and the investigation of evidence or any piece of information that is discovered in digital devices

involved in criminality. It settles cases of disputes/differences where digital evidence is digitally stored [56].

Therefore, digital forensic analysis specifies how results can be gathered from an investigation or examination and also critically analysed in order to derive useful responses and conclusions to the issues or questions reported from previous stages Digital forensic analysis indicates the stages involved in the analysis of the product of an investigation/examination. It provides probative and significance value to a case. Typically, this is where cases are resolved. The product of this phase can result into more examination/investigation or draws a conclusion.

Nowadays, computers and other digital devices are everywhere. They have also, become quite vulnerable in our modern society as they become heavily involved in crime. Beginning from late in 1970s the rate of crime that involves computers has grown rapidly. This creates a need for consistency in the analysis of digital forensic processes and practices in order to keep abreast with the needs of the field and acknowledge new innovations in the field. Digital forensics field has grown rapidly in popularity and support due to the rate at which it is being recognised and accepted in courts. There is a need to analyse the forensic process and procedure so as to measure the rate of success achieved in the field and ascertain its present position and standing [57].

Digital forensics emerged almost three decades ago, and yet some of the pioneers are still steadfast moving on in the field. Some critical components such as targets, people, organizations, tools, and the entire society contributed immensely to this discipline. In the authors view these are: In the second half of the 1900s modern electronic computers evolved and in 1947 became the starting stage of the Industrial age/period of Computing [57, 58] and the age is still on. Particularly, forensic computing or digital forensics concentrates on incidents that were necessary and important to the digital forensic society.

In 1985 the initial documentation on the developments specific to digital forensics were recorded. In fact, the term digital forensic did not even exist beginning from 1960s till the early 1980s only universities, corporations, research centres, and government agencies could own and operate computers because they were used mainly as an industrial device. Literally, they require substantive physical infrastructure, requiring huge amounts of power and air condition. In addition, they also require committed staff that is highly motivated and skilled in processing large amounts of data. The responsibility became the early interest of judicial

and law enforcement agencies in computers and the information security. The first material to describe the use of digital information in prosecution and investigation of crimes committed by the aid of computer systems and devices was described by Parker in 1976.

It is the duty of the system administrators to secure their systems, though not much connected to the wider World Wide Web. Also, system audits were developed to make sure that there is accurate and efficient data processing which at that time was not easily affordable. In fact, these audits formed the initial systematic method regarding computer security. It was assumed that the information collected from audits could also be used to investigate wrong doings [59]. The idea was not totally lost on law enforcement bodies because organizations such as the Internal Revenue Service (IRS), the Federal Bureau of Investigation (FBI), and the Department of Defence, were part of the ad hoc sets of law enforcement agents who volunteered to help other case investigators in the process. They were as well given fundamental training on how to extract information from access logs and stored basically in mainframe and mini computers. They were to work in solidarity with the systems administrators in carrying out their responsibilities. However, it was difficult for traditional managers and investigators to actually understand that computers possess the potential to be both tools and victims of crime at the same time.

He emphasized that government agencies are sluggish in getting involved in this current aspect of digital forensics. Stoll, a Unix systems administrator conducted several investigations where he reconciled two accounting system programs that showed little difference in their usage and understood that large number of computers, and several sensitive systems were being accessed by hackers. He then used his own initiative to develop an approach that was capable of recording the malicious activities of hackers' real time via system administration tools and justifiable number of experiments. At the beginning there was really no committed and dedicated institution or organizations, process or training or even tools particularly developed for digital forensics existed. Only operating system utilities and tools were available and being used by individuals, and ad hoc together with the investigative and traditional scientific problem-solving approaches.

In the early 1980s the emergence of IBM PCs resulted in the escalation of computer technologies and computing. The PCs, were very strong and powerful but relatively had just few applications and so was virtually user-friendly. Ataris, Radio Shack TRS-80s, and Commodore 64s were among the several early computers that enabled users writing program

codes as well as access the hardware and the operating systems internals. These skills were associated with the current IBM PCs and PC-compatible computers. Certain persons like Mike Anderson, and Danny Mares Andy Fried from the IRS; Jack Lewis and Ron Peters from the U.S. Secret Service; Jim Christy and Karen Matthews from the Department of Defence; Roland Lascola, Tom Seipert, and. Some of them were part of the charter members of the Specialists group- International Association of Computer Investigative (IACIS) that was the first organization on record that was devoted to digital forensics. There were several other persons who took up the idea that computers would have a prominent role in criminal investigations. More so, those computers could be relevant sources of evidence in criminal cases. Those persons were so committed to digital forensic to the level that they could spend greater amount of their money and time in acquiring the underlying knowledge of the current computing technologies within digital forensic. This they did even in spite of the unsupportive reactions from most of their agencies to their efforts. It is on record at the FBI Academy in Quantico Virginia that the FBI hosted the First International Conference on Computer Evidence in 1993 and delegates from 26 countries attended. In 1995, during the 2nd (second) conference for International Organization on Computer Evidence (IOCE) held in Baltimore, the International Organization on Computer Evidence was founded [61].

The early days' investigations were actually fundamental because the focal point was on data recovery from standalone computers and it was a major issue then because users were fond of deleting data and re-formatting media including the fact that storage was very expensive. Computing and the Internet were still vague and it was very common for criminals to weaken or compromise computers using dial-up access.

It was reported that cheap computers were used to hack the telephones which was the dimension of fraud at that time. Curious adults and criminals innovated that they may be able to get telephone service for free by hacking the telephone networks and also some degree of anonymity which was formally unavailable [62].

Generally, traditional criminals who maintained their activities using computers and some young people who were anxious to apply their scarce technical skills to illegally gain access to computers and software was the subject of computer crime investigations. The IBM PCs and PC-compatible computers running DOS and early Windows versions became the most commonly affected devices. Several apple products, Commodore and Atari computers were also often encountered. At that time, investigators could only use command line tools and

commercial products which were dedicated to forensic use. Several of them were disseminated among the law enforcement body which included Steve Mare's Maresware and Andy Fried's IRS Utilities, Gord Hama's RCMP Utilities and Steve Choy's IACIS Utilities. These digital forensic problem solving tools addressed specific problems, such as identifying or imaging deleted files. Several later versions such as; Hama's REDX, were capable of performing rudimentary piping and multiple operations [57].

Significantly, PC Tools and Norton Utilities are actually great tools used for performing digital forensics. They are commercial products developed for file management and data recovery. At that time almost all the training on forensic uses both of them or either one of the tools, so that certified to be efficient. In 1991, SafeBack was created by Chuck Guzis, it is another noteworthy product which was created to acquire forensic images as evidence. One of the earliest commercial digital forensic product developed was, Safe Back. In the early period, digital forensic specialists performed their investigation conveniently; then there was no record of purpose built laboratory due to lack of funds. Even the large law enforcement agencies rarely have funds. At this period, knowledge of digital forensics was still new and also experiencing conflict indirectly with the criminal investigators that were operating within the area. Criminals were operating across states, cities, and nations freely in communication on criminal activities could only be done directly among peers in different locations whenever possible [57].

However, it was emphasized that several agencies saw the importance of digital forensic capability and decided to implement it. The outcome was the he IRS that developed a program for the Seized Computer Evidence Recovery Specialist (SCERS), and the U.S. Secret Service came up with Electronic Crimes Special Agent Program (ECSAP), followed by the FBI with Computer Analysis Response Team (CART), including the U.S. Air Force Office of Special Investigations coming up with Computer Crime Investigator (CCI) Program which metamorphosed into the Defence Computer Forensic Laboratory (DCFL). All these agencies embraced different methods of training, selection, and operations depending on their various structures and cultures [57].

Often times, individual officers with little training use their own equipment to conduct a lot of digital forensic investigations outside supervision or authorized quality control. The digital forensic body continued to record and sustains reasonable growth in spite of all possible conflicts.

A lot of underlying efforts were witnessed to gather, talent, resources, and knowledge together with IACIS. More so, the Forensic Association of Computer Technologists (FACT) located in the Midwestern United States, designed opportunities for training alongside network practitioners in the field who are located in different places, so that the efforts in improving the standards and quality in the field may be on going. Also, forensic practitioners from the FBI, and the U.S. Secret Service in collaboration with the Maryland State Police and Baltimore County Police in Baltimore began an ad hoc organization which they called "Geeks with Guns". They did this in order to keep developing the structure of digital forensic technology. Furthermore, Forensic Computing Group (FCG) was created in the United Kingdom by forensic practitioners from several law enforcement agencies within coverage of the Association of Chief Police Officers (ACPO). During this time the High Tech Crime Investigation Association was formed. The other organizations and several of the bigger law enforcement agencies started giving forensic training to security practitioners who were interested. Slowly, there was a huge rise in the demand for affordable quality trainings far exceeded the availability. This has been the situation experienced in the field of digital forensics since its invention till date. At that time the academic community did not express any interest in the field, but persons like Gene Spafford, from Purdue University and Dorothy Denning from Georgetown University were two remarkable exceptions. Both professors showed vehement interest in the field and because of that they motivated a lot of other researchers and students including law enforcement agents to become involved in the movement of this promising field [57].

The decades following has witnessed remarkable advances in digital forensics field. The significance of this growth was expressed in how computer systems suddenly turned ubiquitous, cell phones became essential products and the internet became a global component. Prior to this time, most of the voice calls were made through the landline telephony, several computer network connections were through dial-ups and the internet was still not known by so many people. However, going to the end of the early stage of digital forensics, it was most likely that almost everyone not only had heard emails but also owned an email address, a cell phone, and there was heavy reliance on the internet. Most homes and businesses own networks. Significantly computer technology was virtually incorporated in every aspect of daily life and activities which includes consequently, criminal activities [57].

In 1993, George Stanley Burdynski, Jr. case of child pornography significantly erupted. The online undercover operator called Innocent Images used in trafficking illegal images of

minors was discovered in 1995 while investigating the case. Because of this the FBI decided to set up distinct child pornography task force in almost half of all FBI offices some years later. A lot of other law enforcement agencies also run their separate task forces so as to fight child pornography cases. The current violation resulted in the seizure of volumes of digital evidences which showed a large growth rate in the digital forensics technology [57, 63, 64].

More so, the events of September 11, 2001 sky rocketed the digital forensic files and the entire world. Computers may not play significant direct roles in the major hijackings but during investigation, the investigators definitely will discover pieces of relevant information and evidences on a lot of computers across the world since the terrorists also use computers in the same pervasive manners as everybody else. This resulted in the large increase of the amount of; money, time, resources, and personnel dedicated to digital forensics [57]. Consequently, training digital forensic practitioners become very important as technology gets sophisticated. Now the field has become very specialized as distinctions being drawn between, video, digital, audio and implanted devices such as; cell phone which requires specified knowledge and training, and extra storage media and network focused forensics. The two fields are beginning to diverge at some levels, because the study of network intrusions became more complex than ever. Apparently, individuals are no longer driving the digital forensic discipline rather it is driven by law enforcements agencies, government agencies, and professional institution [57]. The efforts to improve and authorize digital forensics discipline have improved tremendously. Between 1999 and 2000 the IOCE, G-8 High Tech Crime Subcommittee and Scientific Working Group on Digital Evidence (SWGDE) published several digital forensics articles and principles [57, 65][67, 68]. The Directors of the American Society of Crime Laboratory – Laboratory Accreditation Board (ASCLD-LAB) have gone across ordinary principles to work in collaboration with the SWGDE in order to accept digital evidence as a laboratory discipline.

Moreover, the FBI's North Texas Regional Computer Forensic Laboratory created the first ASCLD-LAB that was an accredited digital forensic laboratory in 2004 [57, 69, 70]. Thus, forensic tools have undergone and emerged as the earlier "command line tools" turned into a much more complex, graphical user interface tools-suites. The first of the current tool is the Expert Witness tool. Andy Rosen invented this product for Macintosh forensics which later emerged into EnCase. EnCase, and Forensic ToolKit (FTK), became the successors and are now recognized as standard commercial forensic tools.

Several U.S. Government agencies such as the FBI have started tasking themselves to design tools and made breakthroughs in developing the Automated Case Examination System (ACES) and IRS's iLook tool which recorded market success.

In order to add to that, the open source body developed the Linux tools which include Autopsy Browser, Helix, and Sleuth Kit that showcased a matured digital forensic technology process. That gave rise to the formation of the traditional forensic laboratories which offers examination for digital Forensic process, and services were no more provided by different bodies, it became organized in bold formation of structures. An example is the Department of Defence that designed their own central Defence Computer Forensic Laboratory (DCFL) in order to provide forensic services to the law enforcement, intelligence and the U.S. military operational demands [58, 71]. The joint local, state and federal law enforcement laboratories constellation was created by the FBI called "Regional Computer Forensic Laboratories" (RCFLs) to solely conduct digital forensics investigations [58, 72]. Each and every one of the laboratories offered their services to a particular geographic area and they operate based on the standards of ASCLD-LAB. In addition, the U.S. Secret Service in reaction to the developments formed a joint network of Task Forces for Electronic Crimes which was a highly effective component of the New York security system [72]. Each of the task forces is made to supply forensic and investigative services respectively within their area of operations.

However, since 2005, digital forensics has recorded a huge growth and has also forensic practitioners who have been highly equipped to perform different and complex examinations that involve huge amounts of digital evidences. In 2006, the United States Courts adopted new Rules for Civil process which particularly defined digital information to be a new type of evidence and also implemented a system, called electronic discovery (eDiscovery) to handle digital evidence [57, 73]. Still advancing, the FBI made a wide declaration in their congressional testimony that more than 2.5 petabytes of evidence was examined by their Computer Analysis section in 2007. The workload for the traditional law enforcement agencies became drastically reduced. Today, Information security practitioners and professionals have acknowledged that the field of digital forensics is a core critical skill area. The law enforcements and the digital forensic practices differ in their objectives and needs but look alike in the tools used and the general concepts. Nowadays, there are academic degrees for digital evidence professionals and practitioners including several authorized and

recognized formal training and a lot of certifications. Presently digital forensics is recognized as a career enhancement which was not available and obtainable a few years ago [57, 74].

Digital forensics has continued to be embraced across the globe within the academic fields. Universities and colleges have accepted and recognized the potential of digital forensics including its demands. Though research funding for forensic education is still lacking across the world, forensic education is gaining popularity. Up till now so many universities and institutions of higher learning across the world have not being able to include digital forensics in their curriculum in-spite of the great demand for the knowledge and expertise. Recently the U.S. Forensic Education Program Accreditation Commission (FEPAC) made the first bold step in accrediting academic programs in digital forensics in the U.S. Still advancing up, the American Society of Testing Materials (ASTM) Technical Committee (E30) has also created a draft of the standard for digital forensic education and training programs for all digital forensics learning institutions in the U.S [57, 75].

Records show that, the Digital Forensic Research Workshop (DFRWS) has been taken place for about ten years since it was formed. The International Federation for Information Processing (IFIP) Working Group 11.9 on Digital Forensics is also in its seventh year. Recently, the International Conference on Systematic Approaches to Digital Forensic Engineering celebrated its fifth anniversary. Now almost all devices that use electricity have some form of digital storage and this indicates some advancement and maturity in the materials being examined. All networks, wired or wireless, connect so many of the devices that we utilize in our daily lives. This then forms the drive to create several networks and also web-based operations and services, which includes cloud computing. Several services, like Facebook and Twitter, are continually changing the manner in which people interact and communicate. These impacts and changes are also starting to align with how digital evidence is being collected. Nevertheless, E-mail has featured as a prominent source of information and this has accelerated into a huge challenge for forensic, information security and management [76]. 35

The wealth and impact of academics in digital forensic field can be measured by the number and quality of conferences offered. This up shoot is as a result of the huge increase in the demand for services rendered by digital forensics.

Digital forensics is really a complex field and a continuously evolving field. Its practitioners and experts are now better educated and have quality training [57]. Forensics are no more a

linear process that is focused on data recovering, but rather a knowledge evidence-based management process which are being incorporated into intelligence analysis, information security, electronic discovery and investigations. Digital forensic technology in anticipation, envisages that more educators and researchers, managers and practitioners will embrace the field in the near future. However, criminals and hackers are not also relenting; they are getting more educated, organized, and funded as well. Also, they have embarked on joint and distributed efforts because their access value and information band grows alongside the society's reliance on the technology and information infrastructure. Thus their payoffs are very significantly large, as safety and security are constantly threatened. At all times everyone (and their information) everywhere is at risk. All devices and systems are constantly under attack [57, 60].

Consequently, digital forensic technology is improving in its tool development in order to combat these threats which are on the increase The advances are towards automation in tools with; in-built analytical capabilities, allowance of necessary items to be recognized without viewing each and every item, including conducting data recovery. Most of these tools are semiotic, understanding human language and human communications, and also have the ability to interpret content and context. This is indeed a great innovation with strength in accreditation, and strong individual and quality management certifications. These reported results assure the society that the information obtained and the conclusions arrived at is quite reliable [57, 60]. Therefore, one of the objectives of this research is to advocate these results and solicit for organizations to cooperate with each other and also support interoperability and integration of digital forensics and systems-especially biometrics processes, people, and tools. If this becomes the global concept and challenge, then more stable and international legal standards will emerge.

The two concepts are separate fields that are getting large positioning on a daily basis. They have a wide range of customers who strongly cling to the technology. Therefore, there is a need to establish a link for interoperability between digital forensic and biometric technology, as interoperability is one of the requirements of any information security standard [57, 60] However, in all the above highlighted studies, the digital forensic technology has been widely applied in several contexts and much has not been applied in biometrics context especially where biometrics is used for access control.

Obviously, the digital forensic market is expanding and the institutions and organizations that adopted and implement digital forensic practices and employ its practitioners as well as those who depend on them are developing. Every institution utilizing digital forensics is challenged to embark on biometrics technology for verification and authentication. This will place forensic technology into delivering more efficient tools for the identification of impostors involved in biometrics authentication systems via digital forensic technology tools. Digital forensics will thrive most when biometric features are involved in crime investigation and examination.

2.3.2 Developments in Biometric Technology (BT)

In this section, we explain how biometric technology came about. The section incorporates an overview which describes the history of BT.

The term "biometrics" emanated from Greek and it can separate it into two aspects, bio and metrics: "bio" which means life and "metrics" which means to measure [77, 78, 79, 80]. Biometrics is based on the anatomic uniqueness of an individual that can be used for identification. These unique characteristics can be used on automated access control systems to prevent unauthorized access by checking unique physiological features or behavioural characteristics submitted with the one previously captured in the database to identify an individual [77, 78].

The first evidence of Biometrics was originated many years ago when the cavemen administrators conducted an experiment on the systemized process of providing food to the workers during the building of the great pyramid of Khufu. They made records of information about the workers such as name, age, work unit, position, and occupation. He discovered later that they were cheating him, so he decided to also record both the physical and behavioural characteristics [78].

As far back as the 14th century the merchants in China used biometric authentication in a way that was significant among the merchants when they easily used paper with ink to collect footprints and palm prints of children in order to recognize each and every one of them and also differentiate one from the other. It was really interesting where and how biometric started and it is still in development becoming the most popular and widely accepted [79].

A Czech biologist and physiologist called Jaonnes Evangelista Purkinje, was the first person who managed to group fingerprint patterns during her study of papillary ridges of hands and

feet published her scientific work in 1823. A British officer who lived in India, Sir William James Herschel, in 1858 was the first European to use his fingerprints for identification. He believed that they were unique so he used them to sign documents. Also, in 1870 Alphonse Bertillon, as an anthropologist, he was searching for how convicted criminals can be identified used both palm prints and footprints including body movements and several forms of marks on their body. The idea was referred to as "Bertillonage", became very popular and was adopted in American and British police forces and this helped to minimize the circle of suspects [80].

Apparently, Henry Fauld was the first European who insisted on having some meaning of fingerprints used in criminal identification when he required explanations for a system to classify fingerprints, and produced very similar classification systems. Furthermore, Sir Francis Galton in

1892 published a book titled "Finger Prints" where he categorized and described three main fingerprint patterns as loops, whorls and arches. He proposed the use of all ten (10) finger prints. The use of biometrics especially the fingerprint continued to become more and more popular when a Bertillon system encountered a difficulty in identifying two identical twins, until 1903 when New York State Prison officially adopted a regular use of finger prints in United States (US) in criminal identification. In 1904 it was adopted by St. Louis Police Departments in Kansas. Subsequently, the US Army adopted it in 1905 and in 1906-the U.S followed suit. Also the U.S Marine Corps used the fingerprints identification in 1908. Hence, the first automated use of fingerprint system was originated in the 1960s. It was adopted by the Federal Bureau Investigation (FBI) in 1969 when they tried to automate the fingerprint identification mechanism [81].

Meanwhile, Lesk and Harmon together in 1965 created the epoch of face recognition where the eyes, nose, mouth, ears were located in photographs. Building on this, by 1980, they used Twenty one (21) markers as the colour of the hair, and the thickness of the lips to automate face recognition systems. It is recorded that the first hand geometry system was used in 1974, which gave rise to the signature recognition systems created by Standford Research Institute and National Physical Laboratory. Consequently, biometrics came into full use the 1980s as an automated measure of identification.

By 1983, the U.S Department of Energy began conducting several experiments on biometrics at Sandia National Lab and also the Department of Defence started the same experiments at

Naval Postgraduate School. Still developing the biometric technology the Department of defence in the Naval Postgraduate School designed the first retinal scanning and in 1985 which was used as an access control to secure access within the institution. Slowly the state of California adopted fingerprints for all drivers' license applications [76, 11, 78].

Consequently, as the use of biometric technology was gaining ground, the first biometric association was formed in 1986 in the US called the International Biometric Association. Daugman of Cambridge University came up with the iris recognition technology in 1990. The United Kingdom formed the Biometrics Association in 1991. The U.S. instituted the boarding system in 1994 which was determined by hand geometry, and consequently in 1997 the first Biometric Testing Centre was established and that gave rise to the deployment of the first biometric procedures and standards in 2002 [82].

However, to date the use of biometric has continued to increase as systems and network developers have discovered its functionalities which include Universality, Uniqueness, Permanence, Measurability (Collectability), Performance, Acceptability, and Circumvention. Universality- implies something that each and every one possess; Uniqueness- implies something that distinguishes one person from the others; Permanence (biometric measurement should be constant over time for each person); Measurability (collectability) (it should be easy to measure, should not demand too much time and cost); Performance- implies that speed, accuracy and robustness; Acceptability- implies how well people accept biometrics; Circumvention- how easy it is to fool the system. As the value of information systems and networks grow rapidly, the use of digital forensics and biometric technology becomes inseparable from our daily lives because it provides a means of readiness to two kinds of attacks such as: privacy attack and subversive attack. When the attacker gains access to the data to which he is not authorized it is referred to as privacy attack, and when the attacker gets the opportunity to manipulate the system files and disrupt the network it is referred to as subversive attack. Therefore, integrating biometric authentication will promote digital forensic technology by facilitating fast data analysis, easy evidence discovery, and also provide accurate identification of suspects. This will contribute in combating cyber – crimes and cyber – attacks [11, 43].

2.4. Different Biometric Features

There are several biometric features that exist; some of them have already been adopted in commercial systems while some are still under investigation. Some of the existing biometric

features include; iris, face, hand, and finger geometry, hand or finger vein, voice, signature, palm prints, finger print and signature [52].

i. **Iris:** This type of feature is very distinct for every individual and every eye (Daugman 1999). Every human iris has a visual texture that is determined by the chaotic morphogenetic process which takes place in the embryonic development. The capturing of the iris image is done via a non-contact imaging process. This is usually done by the users' corporation to ensure that it is properly registered and also captured at a predefined distance from the camera's focal length. This iris identification technology is fast and accurate when the iris captured images are on high resolution.

ii. **Face:** The face biometric has a high acceptability. This is because people mostly use it in their daily visual interactions. Moreover, a nonintrusive method is used in acquiring face images. Most times this type of biometric trait suffers from face disguise when the recognition applications are unattended. It is usually challenging to design face identification technologies that can tolerate/accommodate the effects of aging, posture, expressions, and various image captures using the camera.

iii. **Hand/Fingerprint Geometry:** Human hand features which Include: the various lengths of fingers, are not very distinctive but are relevantly peculiar and invariant to every human being. The mode of image capturing/acquisition requires the subject's cooperation in order to properly capture the front view of palm images put on a panel together with fingers stretched out. The hand's requirements for template storage are very small which makes it very suitable for systems whose bandwidth and memory are limited. Because its distinctiveness is limited, they can be used in verification systems only but not in identification applications and systems because of its distinctiveness which is limited. The finger geometry systems and applications measure a maximum of two fingers geometry instead of the entire hand; therefore, its compact size makes it preferred.

iv. **Hand and Fingerprint Vein:** The hand vein structure is determined using the infrared/imaging to scan a clenched fist at the back. Detection of vein structure can be done as well in a finger with rear infra-red sensing. The devices or systems that are used in capturing the vein utilize infra-red light that emits diodes that are

inexpensive (LED). This is giving birth to hand and finger biometric commercial systems.

v. **Voice:** This type of biometric system is the only feasible biometric trait that requires identification over the telephone. Voice capturing is unobstructed and it is not meant to be sufficient in distinction to grant every individual's proper identification in a large database. Even condition of someone's health like; stress, cold, or emotional state also affects the voice and even mimicking of others by extraordinarily skilled people also affects voice identification traits.

vi. **Signature:** This type of trait or characteristics has been widely accepted by the government in commercial and legal transactions as a mode of identification. It has been proven that the way people sign their names varies among individuals. Signature as a behavioural biometric is usually affected by physical and emotional conditions. This makes it subject to change over time. More so, people who are professionals in forgery can reproduce signatures of other people.

vii. **Fingerprints:** Fingerprints are highly distinctive and also permanent, even though they are capable of slightly changing temporarily over time, because of the bruises and the cuts on the skin. They also reappear when the finger heals. Fingerprint scanners can capture live scan quality fingerprint images with ease and without any issue of segmentation within the background. However, they are not recommended for surveillance because life scan fingerprint scanners are not able to capture a fingerprint image at a distance without the knowledge of the person. The adoption of automated fingerprint identification systems has made fingerprint scanners become convenient and also affordable. They are used in forensics for criminal investigations to identify fraud, and security traits. They are also the most robust biometric technology that is appropriate for a broad range or huge number of applications for identification. Latent fingerprint images are the type of fingerprints collected at the crime scenes and they are regarded highly and are important for forensic applications. Chemical techniques are used to lift the impressions of fingerprints that are left on every surface that any finger touches.

viii. **DNA:** DNA is an abbreviation for deoxyribonucleic acid. The nucleus of all cells carries DNA making it a highly suitable biometric identifier that is capable of representing physiological characteristics [80]. The structure of DNA in all human is

very unique because it comprises of the genes that establish physical characteristics like hair colours or eyes. The only exception to this is identical twins. The samples of human DNA can be obtained from several sources such as finger nails, saliva, hair, and blood samples. DNA identification requires that firstly samples or sources that are capable of amplifying it be isolated from possible contamination to avoid the creation of multiple copies of the target sequence, next is the sequencing that generates the unique DNA record. DNA comparison/matching are very popular for law enforcement forensics and applications. Currently, not all the levels of DNA matching can be automated and results can be contested when the process is not properly conducted or the DNA samples get contaminated. In summary, the DNA matching process is time consuming and quite expensive but realistic. Hence, it is not yet suitable for civilian use as wide scale biometric applications [80].

Biometric systems using face, fingerprints and iris recognition has been on the increase over the past few years. Such interest has been substantial with various large-scale initiatives from governments and other sectors that seek to incorporate biometric technologies for the purposes of identification and verification. The biometric technology offers reliable and convenient solutions to the problems of individual recognition. Thus, fingerprint verification and identification system is the most widely used today because it can easily be implemented and it has a high reliability This increase in the use of biometric system in several organizations is a reflection of the increasing security concerns of the individuals involved. The friction ridge and valley patterns of every individual's fingertips are very unique to such individual. For ages, the matching of bifurcations and major points of ridge endings is been conducted by law enforcements in classifying and establishment of identity. Fingerprints are quite distinct and very unique for every person's finger. The most available commercial biometrics technologies, fingerprint recognition systems and devices for laptops, and desktop access are now available globally from several vendors at affordable prices. Users of these devices, are no more required to type passwords, instead by just a single touch access is instantly provided [81]. 42

Fingerprint technology has gained wide acceptance over a period of time as giving accurate personal verification and identification systems because it uniquely identifies a person, is permanent and it remains unchanged. Therefore, every biometric system should include these qualities:

- Universality: The characteristics or traits should be possessed by everyone
- Uniqueness: It should be unique characteristics
- Permanence: Those characteristic should not change with time
- Robustness: Those characteristics should be consistently measured and evaluated

Biometrics systems are reliable when compared to other identification solutions and applications because it authenticates a person's identity using unique physical characteristics instead of other identification measures. Therefore, this thesis supports the interoperability and integration of digital forensic and biometrics to help identify criminals and impostors which are increasing on daily basis. This goal is achieved by providing a detailed analysis of digital forensic process components and biometrics authentication system functionalities in order to provide an effective, reliable and efficient security system that ensures quality of service [82].

2.4..1 Fingerprint Identification

In fingerprint identification, fingerprints are collectively used in referring to human fingers impressions. Fingerprint identification can be operationally divided into three basic tasks namely; fingerprint acquisition, fingerprint classification and fingerprint matching. Basically the acquisition of fingerprints is done from the impression of the ridges and the furrows. Fingerprint classification allocates certain categories of fingerprints to specific fingerprints according to the configuration of the global ridge and furrow. Fingerprint matching determines if two fingerprints belong to one finger [83]

One of the most valid personal identification mechanisms that are very reliable is the fingerprint.

Most of the automated fingerprint identification systems are used in forensic applications [84, 83]

Fingerprint identification has existed for ages since the History indicates that the ancient people recognized and acknowledged the individuality and uniqueness of fingerprints despite the absence of scientific standards. Nehemiah Grew, in 1864 reported scientific studies on the furrow, structure and ridge of fingerprints as expressed in Figure 2.2 [84, 83].

Figure 2.1: Dermatoglyphics drawn by Grew [83]

From that time on a lot of research has been carried out on fingerprints. In 1788, Mayer conducted a research where he described anatomical formations of fingerprint ridges for identification and classification as expressed in Figure 2.2 [83]

Figure 2.2: Fingerprint Drawing by Mayers [86] 44

The first fingerprint classification mechanism where fingerprints were classified into categories according to its ridge configuration as shown in Figure 2.3, (103) were carried out by Purkinje in 1823. The individuality and reliability of fingerprint was scientifically suggested first by Henry Fauld in 1880 by his personal observation [85, 83].

Figure 2.3: Fingerprint Classification by Purkinje [83]

Herschel's discovery and practice of fingerprints helped to establish the basis of modernized fingerprint identification. Francis Galton performed an extensive study on fingerprints late in 19th century [87]. From this extensive study emanated the minutiae features of fingerprint classification. The two Indian assistants of Edward Henry established "Henry systems" for fingerprint classification [85, 88].

Early in the 20th century, fingerprint formations became more accepted and established. Hence, fingerprints are now well summarized and established such that individual person's furrows and epidermal ridges have separate characteristics for different fingerprints. The types of configuration vary according to individuals within the allowed limits that enable systematic classifications. The configuration and minutiae details of the individual's furrows and ridges are permanent and do not change. In the early 20th century, fingerprint verification and identification was formally accepted as a valid identification method and was also adopted as standard routine in forensics [85]. This led to the set up and formation of fingerprint identification agencies and databases worldwide [85]. Various fingerprint identification techniques which include; acquisition of latent fingerprints, classification of the fingerprints, and fingerprint matching techniques were then developed and established. An instance is the FBI fingerprint identification unit which was instituted in 1924, with a database containing about 810,000 fingerprints [89].

With the rapid rise of fingerprint identification in forensics, and operational fingerprint databases, manual fingerprint identification is getting obsolete. Currently, the fingerprint identification database has over 70 million fingerprints compared to the previous/original number which was 810,000. Thousands of identification requests are received on a daily

basis such that a team of above 1,300 experts are not capable of providing real time responses to the daily requests [85].

Since the 1960s, a lot of resources have been invested to develop an efficient automatic fingerprint identification system (AFIS) [85, 83].

Based on the way human experts conducted manual fingerprint identification, the three major components involved in the design of AFIS which includes; Local ridge characteristics extraction and ridge characteristics pattern matching and digital fingerprint acquisition were established. The effort was successful as so many numbers of commercial AFISs are currently installed and they are in operation used by law enforcement agencies all over the world. The operational processes and agencies have been improved greatly as well as reduced the hiring and training of human fingerprint experts. However, the rising demand in the ever increasing electronic interconnected society for automatic personal identification (API) and the success of various AFIS installations applied in forensics have steadily advanced above forensic applications to civilian applications. Presently, identification using fingerprint biometrics systems are widely accepted to have become almost the synonym of biometric systems [89].

2.4.2 Fingerprint Acquisition

Whether the process of acquisition is online or offline a fingerprint may either be a live-scan fingerprint or an inked fingerprint. Inked fingerprints are used to show if a fingerprint image is acquired from an intermediate medium like paper or from an impression of the finger. Inked fingerprints are generally obtained using the rolled method which is referred to as rolled ink fingerprint as shown in figure. Traditional or manual capturing of rolled fingerprint images undergoes several steps which initially includes typically placing a few drops of ink on a slate and rolling it using a roller until only a thin layer of the it remains and then the finger is rolled on it from one end of the thumb to the other end on the slate such that the ridge pattern ink comes on top of the entire finger. Next, the finger is rolled against a piece of white paper so that the ridge pattern ink impressions of the fingers appear on the white paper. Lastly, the fingerprints are collected electronically by scanning using video cameras or optical scanners to form rolled digital fingerprints. This ink rolled method of acquiring fingerprints has been the most popular method of acquisition for well over hundred years. Fingerprints acquired through this method generally have a large area of valid furrows and ridges, but can record several deformations because of the built-in design of the traditional

manual rolling process. [89, 83]. Quality control is usually a challenge because a direct feedback to control the acquisition process is not available for the subject. This process is also slow and cumbersome.

In forensic applications, great interest lies in the latent fingerprint. Perspiration exudations of hidden pores on the ridges of fingerprints and continuous contact of the finger with several objects and other parts of the body leaves a film of grease or moisture on top of the finger and the surface of every object it touches. This implies that once the grease or moisture is transferred, an impression of the ridges is left behind. Latent fingerprints are essential in forensic investigations and analysis [85, 83].

However, the live-scan fingerprint image is the type of fingerprint image that is acquired directly from a fingerprint device electronically without going through the process of the traditional manual process of obtaining impression on a paper. This method uses a mechanism of sensing through the ridges and the furrows of various impressions of the finger. Those mechanisms include: (i) Optical frustrated total internal reflections, [89]; (ii) Ultrasound total internal reflections [90]; (iii) Optical total internal reflection of edge lit holograms [91]; (iv) Thermal sensing of the temperature differential (across the ridges and valleys) [92].v) Sensing of different capacitance and non-contact 3D scanning [93, 94]. Scanners that are based on these devices can be used to acquire the fingerprint directly from the human fingers. With this mechanism the intermediate conversion into digitized process is eliminated. This enables the development of online systems if the acquisition methods of the scanned ridge structures of scanned fingers are clear. However, direct feedback on such devices is relatively easy to control the quality of the acquired fingerprints.

Usually, a life scan fingerprint is obtained using a mechanism called "clab". In this mechanism, the person's finger is positioned on the surface area of the device used for obtaining the print. This is done without rolling. The device (scanner) captures only the ridges and the furrows in contact with the acquisition surface. The image and deformations of the actual ridges and furrows appears smaller when compared to a rolled fingerprint image.

The optical frustrated total internal reflection (FTIR) concept provides the most prominent and popular technology that is used to acquire life-scan fingerprint images as shown in figure 2.4 below [95]. When a finger is positioned on one side of the glass platen-prism, the ridges of the finger automatically comes in contact with the platen; whereas the valleys of the fingers that are not in contact forms the assembly of an LED light source of the CCD put on

the other side of the glass patterns. The laser light carriers are placed on the other side of the glass pattern. The carriers of the laser light are placed in such a way that it can produce a reflection of the laser light through the glass. The light that is incident on the plates within the surface of the glass touches the ridges; it randomly scatters as the light incident on the surface of the glass corresponding to the valleys suffers complete internal reflection. This results into the realization of a fingerprint image corresponding to the image on the imaging plane of the CCD. A typical instance is expressed in Figures (2a,b,c).

Figure 2.4a: FTIR fingerprint scanner by Identix

Figure 2.4b: FTIR fingerprint scanner by Digital Biometrics

Figure 2.4c: Simultaneous acquisition of four fingerprints by a multi-finger scanner

2.4.3 Fingerprint Classification

In fingerprint classification, the furrows' and the ridges' global patterns within the fingerprints control region form special configurations. These configurations contain some level of intra class variations which are significantly small and provide space for a systematic fingerprint classification. In fingerprint classification, only a certain area of the fingerprint is given as a pattern area of interest. The fingerprint's pattern area is made up of the ridges that are rich in the type lines and it is determined by the two innermost ridges forming a divergence that goes down to encompass or encircle towards the central area of the device as expressed in figure 2.7, it is an instance of type lines and pattern area [88].

The pattern types of singular points called delta which is called the outer terminus and the core which is sometimes called the inner terminus. The delta is defined as the point of divergence of the type lines. It can be a ridge or a short ridge at or in front of and nearest to the centre between the innermost diverging ridges. Figure 2.5 is an example of delta configuration. The core is referred to as the specific point located/situated within the innermost sufficiently re-curved ridges. The rule that determines the selection of the core is very complicated because of the variations in the formation of curved ridges. The examples of core configurations are shown in Fgure 2.6.

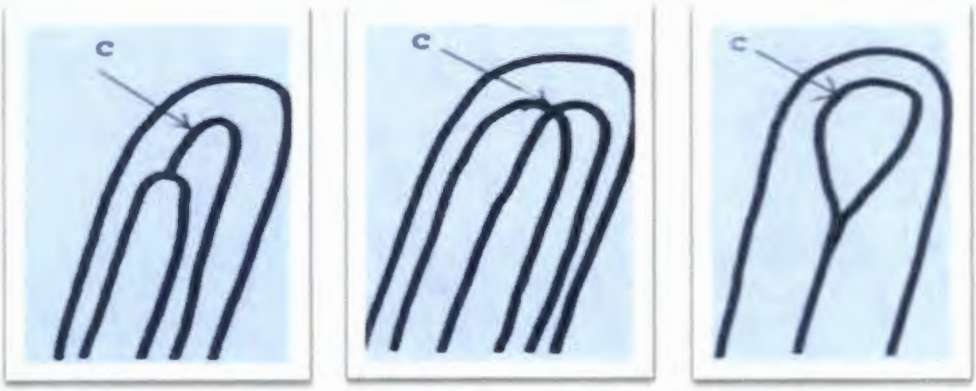

Figure 2.5: Examples of Delta Configuration [83]

Figure 2.6: Examples of Core Configuration [83]

The ridge count is another concept that is important in both fingerprint classification matching that touches or crosses an imaginary line drawn between the core and the delta. It is difficult to define ridge count precisely because of the high complexity of ridge configuration. There are three simple examples shown in Figure 2.7 below.

Figure 2.7: Examples of Ridge Counts [83]

However, we can as well define ridge count as the number between the given parts of minutiae. Therefore, using the above definition of ridge count we can categorize fingerprints as follows: A loop, a whorl and an arch.

i. **A loop:** In this type of fingerprint a maximum of two where at most two deltas are contained with a re-curve, a touch or a pass with an imaginary line passing through to the core. Also it terminates around the same area at which such ridges (ridges) control. There are three major characteristics that determine the loop classification of a fingerprint which include at least one sufficiently curved ridge, a delta, and a nonzero ridge count. Loops can be divided into ulnar loop and radical loop depending on the tendency of the orientation and the fingers. About 60 -65% of human fingerprints belongs to this category [88, 89].

ii. ***A whorl:*** This is the type of fingerprint in which a minimum of two deltas having a re-curve in front of each of them. It is quite a general definition that encompasses the real essence of the categorization. Whorls have four loop, and accidental. The amounts of human fingerprints that belong to this category are about 30-35% [88, 89].

iii. ***Arch*:** This is a special kind of fingerprint which is about 5% of all fingerprints [83]. Arches have two sub groups which include tented arch and plain arch. Presently, human experts and automatic systems still find it difficult to handle classification. Up till now, only a few fingerprint classifications exist.

2.4.4 Fingerprint Matching

Fingerprint category information and other global pattern configuration like the number and position of the core, delta and ridge count may indicate, to an extent, the individuality and unique nature of fingerprints. Its uniqueness is determined exclusively by the local ridge characteristics coupled with their relationships. Research has been able to identify up to one hundred and fifty distinct ridge characteristics [83]. Ridge bifurcation and ridge ending are referred to as minutiae which are the most dominant and popular ridge characteristics. The point at which the ridge terminates abruptly is defined as ridge ending while the point at which a ridge diverges into several branches is defined as the ridge branches. Examples are expressed in Figure 2.8 below.

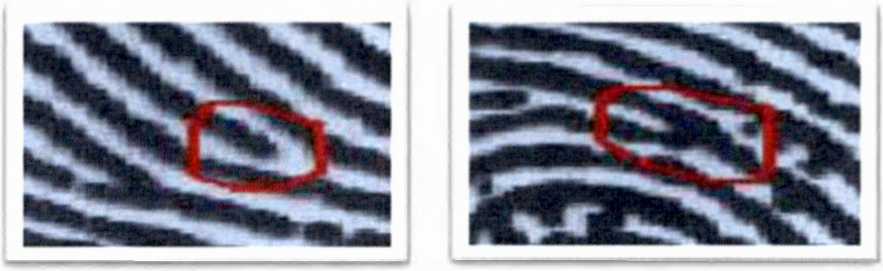

Figure 2.8: Ridge Bifurcation; Ridge Ending [83]

The fingerprint minutiae generally are robust and stable to the impressions of fingerprint. When two fingerprints that belong to the same category with a sufficient number of minute details are identified, then it can be confidently concluded that they belong to the same person. To reliably match fingerprints is an extremely challenging feat due to the huge differences in the impressions obtained from the same finger. The main factors responsible for intra-class variations include rotation and displacement, partial overlap and non-linear distortion, variable pressure and the skin changing conditions, feature extraction errors and noise. For this reason, it is possible to have fingerprints from the same fingers looking different and fingerprints from different fingers looking alike. There care must be taken to ensure dissimilarities.

Several factors are considered by fingerprint examiners and investigators in order to certify the assertion that two fingerprints under investigation come from one finger and that a particular finger generated two sets of fingerprints. Such factors include global pattern configuration agreement, qualitative concordance, and qualitative factors. By global pattern agreement is meant that any two fingerprints should come from one finger type and by qualitative concordance is meant that a specific number of a corresponding minutia should be

seen, a minimum of 12 at least. The standard is according to the United States forensic regulations. Also, the details of the corresponding minutia must interrelate identically. However, fingerprint matching can also be performed manually by defining complex protocols and a well described flowchart [53].

2.4.4.1 Classification approaches for fingerprint automatic matching

Automatic Fingerprint Matching may have three main approaches which include minutia based matching, non-minutia feature based matching and the correlation based matching [53].

i. **Correlation Technique:** Normally, the correlation process is designed to produce a correlation peak of the images at the output level of the system. The correlation can be used to track an image or object of interest. This technique provides an effective mechanism for determining similarities between the life scan fingerprint and the template stored in the database for authentication. It can also be used as the basis for anomaly identification. The discrimination ability of the technique distinguishes between the entire system users' fingerprints.

ii. **Minutiae-based matching:** Minutiae are usually extracted from two subject fingerprints for storage as sets of points in a plane that is two-dimensional. Mainly minutia matching comprises of discovering the point at which the template and the sets of input minutia align which provide the highest number of minutia pairs.

iii. **Non-minutiae feature-based matching:** When fingerprint images of low quality are used it appears difficult to obtain minutia points, whereas, patterns of other features of fingerprint ridges like; ridge shape, and local orientation, frequency, and texture information can be extracted with more convenience than minutiae, though generally their uniqueness is lower. However, fingerprint comparison in terms of features that are extracted from the ridge pattern is referred to as non-minutiae feature-based matching.

2.5 Related Works

Researchers has achieved most important progress over past few years, there are some recent and comprehensive survey on biometric technology. Most previous work was based on the statistical learning or local matching methods. Rajiv Srivastava et al. analysed the performance of fingerprints based on biometric authentication system. In their work they

addressed determination of appropriate key sizes with security issues and determined matching performance for fingerprint [97]. Biometric refers to measures and analysis of individual physical or behavioural traits. Most researches uses biometric technology to realise identification that is more accurate, and verification of individuals are conducted with more convenience.

Previous studies have been conducted by Saraswat and Kumar et al in 2014, where they showed concern in the accuracy, effectiveness and efficiency of biometric fingerprint verification system. They pinpointed that traditional, manual means of checking attendance is difficult and wastes time. This problem made them develop a new system that uses fingerprint verification mechanisms. The authors - Saraswat and Kumar got convinced by the results obtained from their experiments that the use of fingerprint as a measure of verification is very effective. They highlighted in that study that the application of fingerprint verification and authentication is the most popular mechanism that is capable of identifying and verifying individuals whenever security is of major interest. Also stated from their study is that it is very effective, convenient and reliable to use fingerprints as a verification mechanism. This also corresponds with (Shoewu and Idowu) demonstration in their study of Automated Attendance Management System using biometrics. When properly implemented it is expected to produce solutions to time wastage and errors often encountered in the manual system [98]. Previous studies indicated that the authors' work was done on the basis of parameter optimization while a lot of researchers use Genetic algorithm to implement their work [99]. Wavelet statistical features, Fuzzy systems, Geometric prediction, Radial basis function of neural network, and convex hulls, and Principal Component Analysis related to the theory of minutia based algorithm can be used in fingerprint matching whenever there is a possibility of having a fairly bright fingerprint. [97].

The authors of this paper suggested that several mechanisms can be used to control various attacks on the web (internet) and as well listed several measures that can be adopted in order to ensure that the fingerprint template of the user be appropriately protected and secured privacy. In this work, the authors expressed the performance and evaluation of the security measures in a web-based application. The performance and security evaluation of biometric web based application was successfully done [98].

In the security world a lot of threats are encountered continuously from various threats and attackers, from infrastructure or network misconfiguration, from devices enabled, from

simple unavailability, and decrease in the quality of service due to the behaviour of the network which is unpredictable. Most of the world today has become network dependent and as such any loss of network connectivity and loss of services provided by such networks this can be potentially devastating to any business or organization [87].

It is extremely important to secure information system resources by making sure that the resources and services provided are adequately and highly protected. Information security is not about passwords and usernames only. It entails various regulations and data privacy and protection policies. There are some existing proposals on information security management created by international organizations for standardization.

A model that combines security concepts with methods for privacy requirements has been designed. The author employed a typical case study that demonstrates the applicability of the work [100].

More so, a model, using a case study that combines security concepts with methods for privacy requirements has been presented. The authors reported that the essence of information security management culture in every organization, or institution, and company. It provides a guide which information security developers and managers to be able to design information security controls and polies that is best suitable for our today's technology, and end users [101].

Furthermore, network architecture has been developed. This network architecture is suitable for Next Generation Internet (NGI) which can prevent the treatability of any operation and as well as maintains privacy of communication entities while making their individual identities a major network element. Inherently, the architecture accords the mobility and authentication of the various entities participating in the communication. The author exhibited the successful verification of the protocol security and showed its behaviour in order to demonstrate its feasibility and scalability when applied on two different architectures [102].

Moreover, another paper titled -Analysing the Security Risks of Cloud Adoption using the SeCA Model: A Case Study. A single case study was reported in the paper with the description of a huge Dutch utility provider. This was carried out in order to understand the facets of the Cloud and to point out the associated risks with it. The use of the SeCA model is to analyse Cloud solutions and discover the associated risks and having in mind the specific data classifications [103].

In addition, the paper, titled - The Modelling of a Digital Forensic Readiness Approach for Wireless Local Area Networks. It shows the most popular problem with WLAN digital forensics. This problem aims at intercepting and preserving the communications that are generated by the mobile stations and also performs an adequate digital forensic investigation process. The study emphasizes that the availability of digital information can raise the chances of utilising it as digital evidence [104]. This is why the use of biometrics features for systems and network users is supported in this research work to enable an easier and accurate identification. It is an effective mechanism for protecting networks, and various infrastructural devices must be put in place to achieve an efficient quality of service, which is the reason for network security [105]. Therefore, avenues to protect information systems and networks include digital forensic and biometric analysis. Digital forensic technology is not a new paradigm in information technology security. It was innovated barely 40 years ago primarily for data recovery, and has grown into an important part of many investigations. DF tools are readily available and are used on a daily basis by law enforcement agencies, the military, government organizations, and other private business transactions and industries. There have been rapid increases over the past decade in the developments of DF research, tools, and processes because people now rely on it on a daily basis without knowing it. The advent of DF brought a solution to crime perpetrated using computers which includes bank fraud, and phishing, money laundering, and phishing, including child exploitation. Tools for forensic investigation have turned out to be such important information assurance due to their capability to reconstruct cyber-attacks evidence for legal actions [13].

Furthermore, in 1987 Wood et al. communicated the incident of two experts involved in a local data recovery, he worked for 70h in order to recover only a copy of a database file that was largely fragmented and was deleted unintentionally by a careless researcher. [55]. The use of DF was limited because disks had small storage capacity and evidence left on time sharing systems did not necessarily require recovery tools to extract them. It was only a few cases that require digital analysis media for extermination and cyber-attacks were not common.

However, in 1983, the Federal Bureau Investigation (FBI) began a program referred to as "Magnetic Media Program" to boast digital forensic but could only perform three (3) cases within the first year. In 1983 introduced computer hacking as evidenced in the 1983 movie called "war games". Until the Cyber Crime bill of 1984 abuse was passed, Computer hacking was not regarded as a digital crime. The act was passed in 1984, in order to limit the reasons

to subject networks and systems to forensic analysis. From 1999-2007 digital forensics grew exponentially from a data recovery process to one that could recover instant messages and e-mails for the prosecution of criminals [106, 107]. System and network forensics has brought the possibility of envisaging crimes committed several months earlier. Since 2008, digital forensics has gone global and it is so reliable to have left the lab into a television (TV) screen. Consequently, digital forensics is traditionally used in criminal investigations, casualty identification, medical exterminations, network intrusion detections, forensic expert testimony, repositories, consulting services, research and developments. Also it is emerging non-traditionally, in the areas of intelligence, counter intelligence, site exploitation, support to significant investigations, and others in order to overcome the full spectrum of threats and attacks that are on the increase [108, 109].

The Digital Forensics Research Workshop [DFRW] in 2001 proposed a procedure for digital investigations which involves the following six components; Identification, Preservation Collection, Examination, Analysis, and Incident Reporting [20].

The requirements for the next generation DF were reviewed by Ricahard and Reussev in 2008. They emphasized on systems requirements. They argued that CPU cycles are wasted by inefficient system design and the inability to employ distributed computing techniques introduces significant and unnecessary delay. Generally, DF system designers begin every new project afresh. In 2009, Aye during the digital forensics research workshop developed a second generation computer forensics analysis approach. Mocas followed suite to propose a framework that can assist theoretical security measures in digital forensic research. His main goal as presented in the proposal was to define a group of properties and terminologies that can be used to organise the principles for developing and evaluating digital forensic study. His emphasis was that all digital forensic study should be able to put some elements into consideration which include data integrity and context, in which evidence is encountered, authentication and non-interference, and reproducibility including the capability of every proposed technique to meet approved minimum requirement [108].

More so, Pollitt reviewed fourteen (14) different models for digital forensic investigations. A large number of the models depend on the capability to utilise the collected digital evidence appropriately. Moreover, Ray et al developed a proactive digital forensic system that can predict threats and attacks and also change the collection behaviour before the attacks occurs. Adding to that, Brandfordt et al reported a mathematical model that caould decide the

content, effect, and frequency of any proactive forensic incident. He suggested that it is not enough to rely on internal logs and audit trails because digital forensic can be achieved on future systems when they are able to proactively make efforts during preservation and data collection. In 2000, Presley and Noblett, Pollitt presented a proposal for a three level hierarchical model that contains various components for a digital forensic such as; policies and examination, practices, technique and procedures. In 2004, Tushabe and Baryamureeba came up with an integrated digital forensic investigation model, and 2006, Kohn et al developed a systematic framework that supports the collection of evidence for court proceedings and propose a three segment framework that can combine existing forensic models proposed. Von Solms and Grobler in 2009 described the various existing models which relate to a life of acquisition of forensic evidence. Also, Ray and Satpathy Radhan, in 2010, differentiated several models for forensic investigation and presented a proposal of a fusion-based tool for investigation. In 2010 also, Rao, Bhat, Shenoy, Abhilash, Patnaik and Venugopal presented a proposal for a practical framework for digital forensic investigation in flash drives [108]. In 2011, Hassan, Ismail, and Yusoff, came up with a proposal for a computer forensics investigation model (CFIM). In 2011 also, Venter and Valjarevic specified the major predictions of a Digital Forensic Readiness Framework used PKI systems [109, 110, 57].

More so, Nance et al presented an article on digital forensic Agenda. They discussed research categories, topics, and problems in digital forensic and specified six (6) categories for digital forensic research as data volume, evidence modelling, media types, control system, live acquisition, and network forensic [16, 54, 111]. However, this taxonomy requires thorough analysis accompanied by strategic reasoning. It is obvious that there is a need for a better identity authentication mechanism to enable digital forensic analysis. Hence this research project presents DFBA for Information Systems and Networks Security. DF no longer comes at a letter stage in investigation processes after the evidence has been tampered with. Now it comes at the beginning of all investigation processes. It is evident that DF is transiting from traditional services to an emerging and all-embracing and reliable information system and network security. Therefore, in this research we advocate the future of security by integrating digital forensic and biometric features in order to maximize systems and networks services and resources which propagate efficiency and quality of service (QoS).

2.6 Chapter Summary

This chapter consists of a review of related literature in biometrics and digital forensic technology. Additionally, the key terms used in the research work and biometric authentication and identification system components were explained. Also, discussed in this chapter is the development and advancement of digital forensic technology which provides a necessary understanding of the emergence of this field of applied computing. The knowledge from the information provided in this chapter will be used or applied in subsequent chapters to achieve the overall goal of this thesis.

Chapter 3

Analysis of Digital Forensic Technology

3.1 Chapter Overview

This chapter describes and presents a phase which designs digital forensic analysis model as a platform to conduct the analysis of digital forensic technology. The components of DF model were discussed extensively and methodically as the various stages applied in digital forensic technology to implement the widely accepted security mechanisms. Additionally, the framework representing the various components of the model will also be analysed. It also progressed to Fingerprint Forensic Analysis Process, Manual Fingerprint Forensic Process, Major Fingerprint Collection Methods, and Automated Fingerprint Forensic Process. The emphasis was to promote and project digital forensic technology as an effective tool to enhance information security and network management as proposed in this thesis.

3.2 Digital Forensic Analysis Model

The digital forensic process transforms systems and networks into digital evidence, whenever information is required by law enforcement agents or by organizations for internal use. There can be several forensic processes depending on the kind of investigation that is to be performed. The entire purpose of DFAM is to follow a process which extracts systems' or networks' information and transforms it into an understandable and useful form using a forensic tool for the law enforcements or the organizations or institutions that requested [109].

The digital forensic analysis model designed and shown in the figure 3.1 provides a simple and coherent manner of discussing the stages of the digital forensic process in this thesis. It reflects the overall principles of the forensic methodology. Several Forensic models exist but primarily differ based on the type of investigation and analysis to be performed. For example; the Digital Forensics Research Workshop in 2001 presented a proposal on the process for digital investigations process that included six steps as shown in the figure below: Identification, Preservation, Collection, Examination, Analysis, and Reporting. Basically, their forensic process involved four stages such as; collection, examination, analysis and reporting as earlier specified, but they included identification and preservation in their

process diagram but according to them, they are not part of the basic stages involved in the process [20]. 60

However, in order to discuss the analysis of digital forensic technology section of this thesis, we utilize majorly the DF process model shown in figure 3.1 below. Therefore, the significance of this is that every institution and organization is expected to specify the model that is most appropriate for the particular need they intend to address. The figure depicts the several phases involved in the process model designed for the digital forensic analysis section of this thesis.

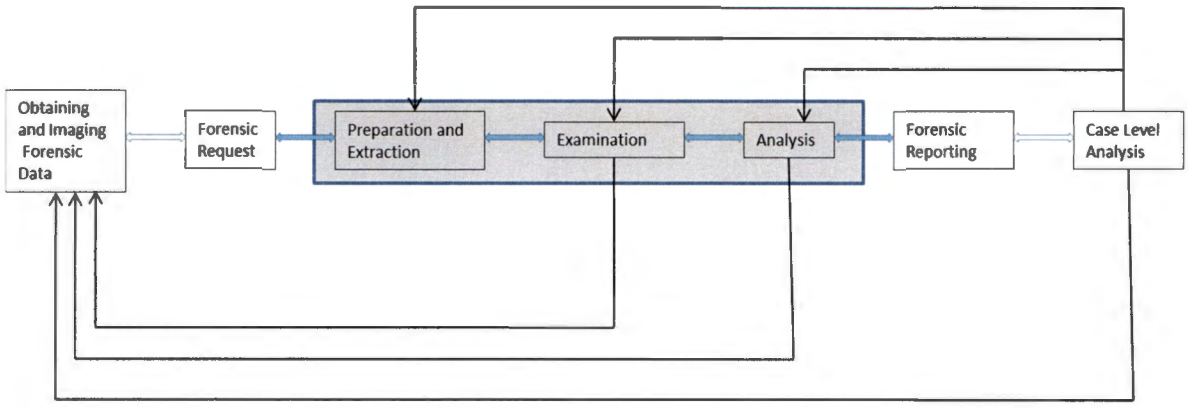

Figure 3.1: Digital Forensic Process Model

The process/methodology as shown in our model entails that the forensic examiner should obtain and image forensic data, obtain a Forensics request, Prepares and Extracts forensic data, identifies relevant data, conducts analysis on the data collected, provides a forensic report and lastly perform case level analysis. The three major components as highlighted in the diagram are preparation and extraction, examination and analysis are core responsibilities of the forensic examiners and must be solely carried out by them. Consequently, all the various components including Obtaining and Imaging, Forensic Data stage, Preparation and Extraction stage Examination phase, analysis phase, documentation phase, Reporting phase, Case Level Analysis are described in details using their respective diagrams shown below.

Typically, the central reason for digital forensic analysis is to determine who may have done what to a system or a network and for prosecution in court. Similarly, the focus point of biometric analysis is also to identify who the impostor, intruder, or attacker is but not necessarily for court presentation, but to ensure that they are warded off and restricted from accessing the computer or network resources. Hence, it is complemented with digital forensic because its main target is discovering the culprit and hand him/her over in court.

Categorically, the exact details can vary depending on the respective organization's policies, guidelines, and procedures. Most times they tend to include certain variations from the normal standard procedures or regulations [112].

The identification process determines who the actual impostor is. Additionally, this section describes the forensic analysis model proposed, designed and discussed in this study. In every investigation, the analysis phase mostly relies on the investigator's skills and it is influenced by experience. More so, this chapter focuses on the innovation of digital forensic especially its advancement into complete automation in investigation and analysis. It also includes its priority towards the deployment of fingerprint (biometric) technology for information security and network management. Figure 3.1 above presents the forensic analysis methodology designed and discussed in this research in order to present its significance and attributes to biometric authentication and identification systems.

Digital forensic analysis emphasizes that for any data collected from a case or an incident to be relevant it must be successfully analysed. Therefore, the forensic examiner or analyst is responsible for performing the analysis either automatically or manually, and gathering information from the extracted data. Also, Digital forensic processes can be significant in extracting biometric (fingerprint) features for more detailed examination and identification of a suspect where a biometric authentication system is deployed [113].

The main idea of Digital Forensic and Biometric Analysis for Information Security and Network Management presented in this thesis is to provide a detailed study of the two security mechanisms, such that every institution, company or organization can be able to see the potential of the two security mechanisms and what they offer. A system may deploy them for a more reliable, efficient and effective security structure that ensures quality of service. Therefore, in this thesis we present BT as a reliable, efficient and effective mechanism that provides maximum security while DFT is also a reliable, efficient and effective detective mechanism that provides exact discovery and identification of subjects under investigation. This study is relevant because both mechanisms are getting wider acceptance and deployment on a daily basis [114].

3.3 Obtaining and Imaging Forensic Data Stage

Obtaining and imagining forensic data is the first component of the model which entails the ability to get the exact copy of the image of interest. For instance, if a violation or intrusion is

suspected in a biometric authentication system or any network, it is advised that the investigator or analyst perform a network traffic analysis and port scanning using network forensic tools like the encase to explore, obtain and document what the perpetrator did or tried to do. If it is identified as a serious issue that requires legal procedures then, the next step should be to obtain forensic request.

3.3.1 Obtaining the Forensic Request Stage

The forensic examiner should adopt the procedures that exist which are followed in securing the rights and warrants from the relevant bodies in order to commence the digital forensic methodology as approved

3.3.2 Preparation and Extraction Stage

The main steps in the Preparation and Extraction stage are shown in Figure 3.2 below. From figure once the process begins the first step is to determine if the forensic request contains what is sufficient to initiate the extraction phase. If not, then the forensic expert should consider restarting by obtaining and imaging forensic data in order to ensure that all possible sources are explored and all potentially relevant data is collected to enable onward progression in the methodology. If the request contains sufficient information to start the process, then the process continues to the setup validation of all hardware and software tools used in the process. It involves making a duplicate in order to verify its integrity. If integrity is confirmed then the requested data should be extracted using the prescribed tools and the data added to the specified list for the phase. If there is no other data to be extracted, then the next Stage should be embarked on. If the process cannot be concluded, then the requester of the forensic process should be informed.

The purpose is to describe the various data sources that are available, and discuss possible actions which the organization and law enforcement can undertake in supporting the collection of data for forensic purposes. Also, the Preparation and Extraction stage makes recommendations on the subsequent ones that the relevant bodies can undertake to support proper forensic processes that align with both legal and internal proceedings [115]. In addition, this phase labels, records, collects, and extracts relevant data or data of interest while preserving its integrity. Preparing and extraction involves preservation and extraction of useful data from the collected using suitable forensic tools while ensuring that the evidence integrity is consistently maintained.

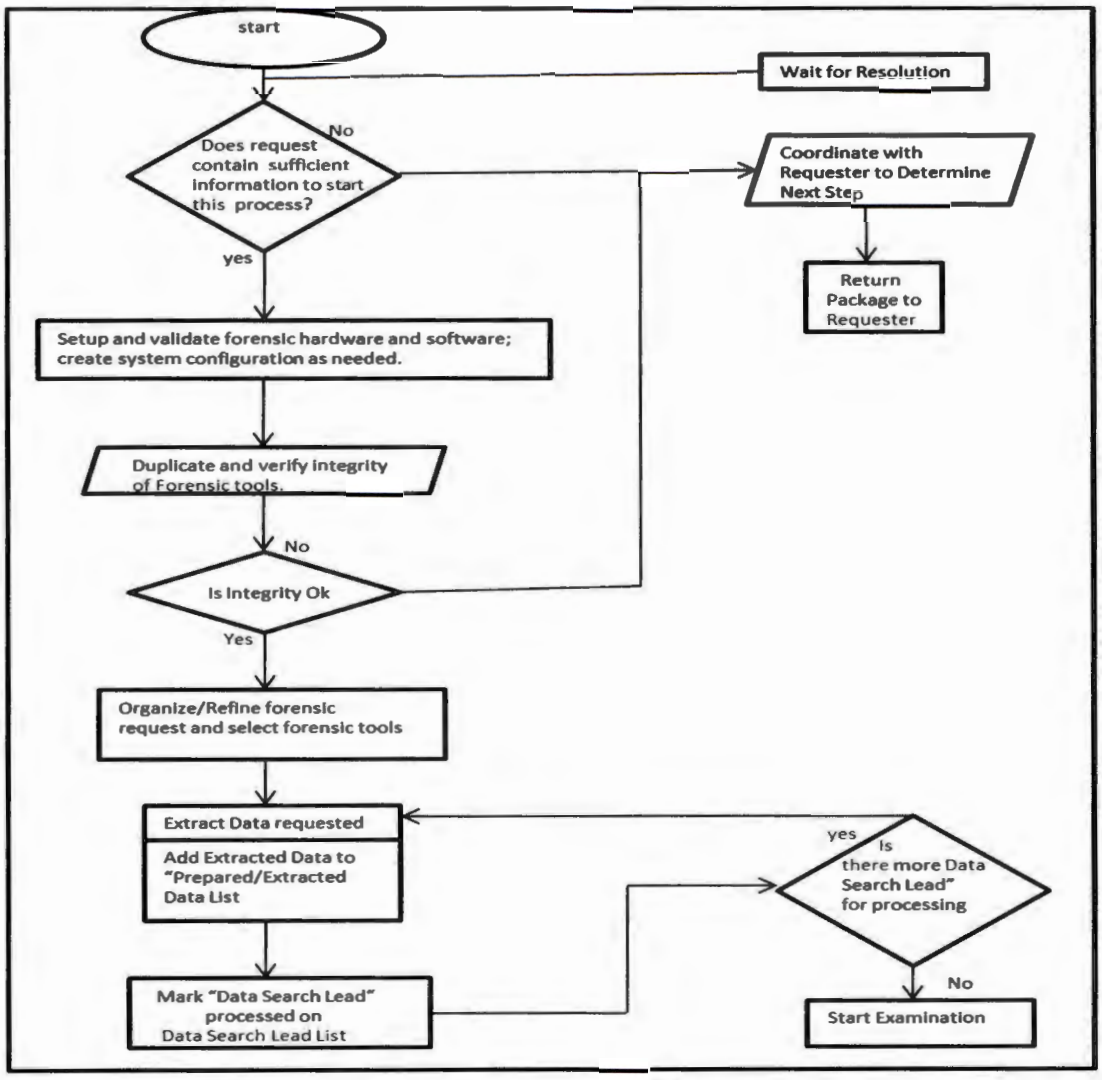

Figure 3.2: Preparation and Extraction Phase

The providers of internet service for any organization have the network logs; therefore, forensic examiners must put into high consideration the owners of the network and the possible effects of the data collection on the system or network. They should also be able to obtain relevant documents for a search warrant putting into consideration the organization's and company's policies that must not be violated unnecessarily, like court orders where necessary. Forensic examiners should utilize attainable possible sources of data instead of unattainable ones which may not be practical [115].

However, once all the relevant data are processed then the examination process should be commenced. Consequently, the steps in examination stage specified in the figure below are followed to ensure that useful data and information are obtained to enable the proper flow in the identification phase [115].

3.3.3 Examination Stage

This is the next stage after conducting the preparation and extraction Stage. At this level, the examiners/analyst will conduct the examination process on each and every item on the Extracted Data List. This phase is diagrammatically explained in Figure 3.3 below.

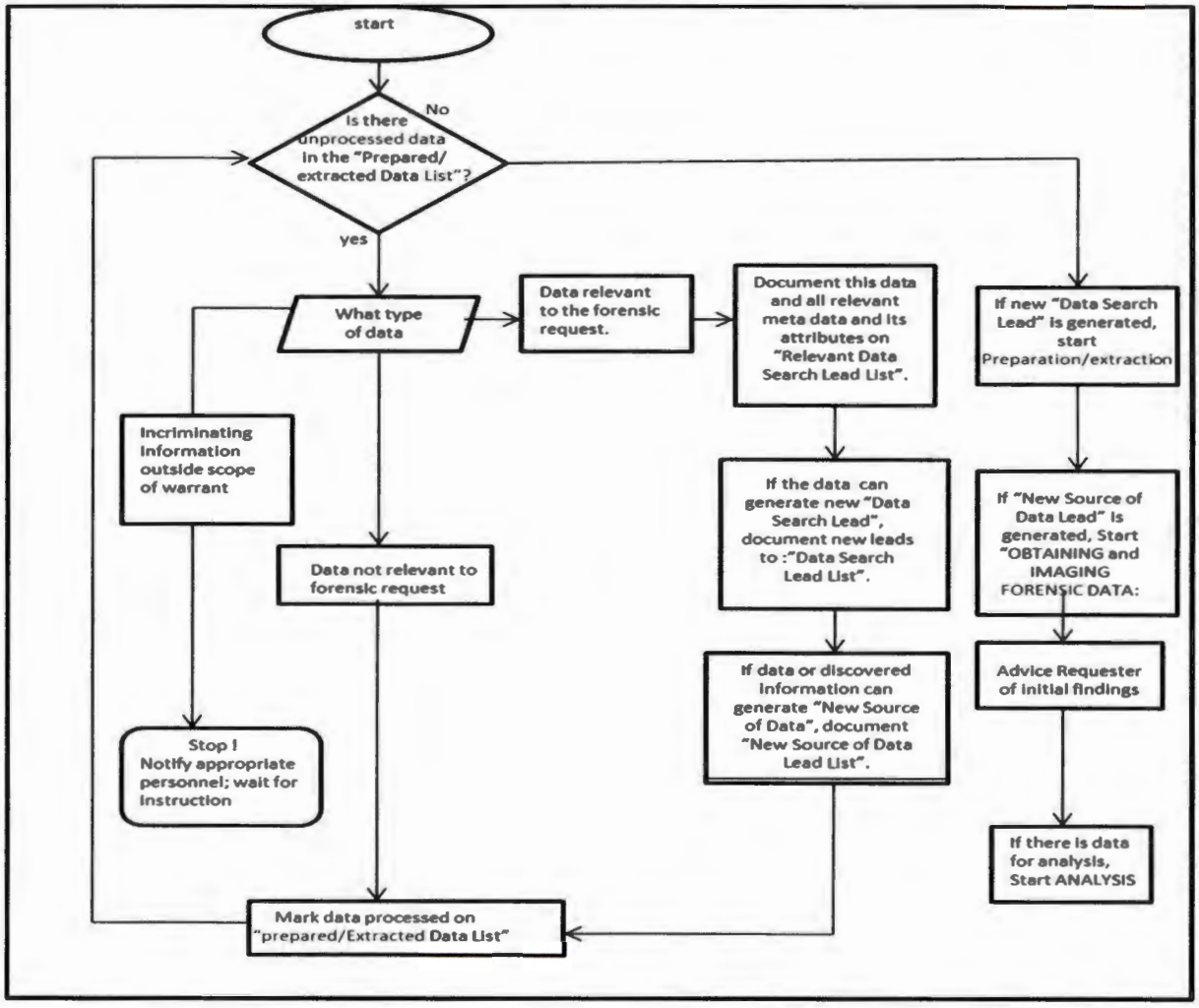

Figure 3.3: Examination Phase

In this Stage the forensic expert examines all the collected data in the extracted data list to determine the type of data and its relevance for the forensic request specified. Following the components of the figure, all the unprocessed data in the extracted data list is identified and the relevant documents are documented and recorded in the Relevant Data List. If other suspicious documents are discovered, it is expected of the forensic expert to stop and notify the appropriate authorities and the forensic requester while the entire process is on hold. But if not, then the process should be continued with all the discovered Data Search Lead Lists and New Source of Data documented. After this, the preparation and extraction phase can be

commenced. The forensic requesters and the relevant bodies should be notified. And when all the extracted data have been properly examined, then the Analysis phase may commence. [115].

During this stage, it is recommended that examiners inform the forensic requesters of the first and previous findings in the process. Both the requester and the examiners will be able to decide together on what they envisage should be the effect and impact of continuing with the new leads on the investment. The examination phase involves close identification of collected data in order to identify relevant pieces of information and in turn extract them. Additionally, those data files that are of high interest can contain a lot of information which may be irrelevant and unrelated, so the files need to be filtered to get hold of useful information. Several tools exist which can be used to filter and sieve the collected data files to identify information of interest.

3.3.4 Analysis Stage

The next stage after the examination phase is the analysis; this involves the evaluating the results obtained from the Preparation Stage extraction and identification phases. Analysis involves examination of the obtained relevant and useful data that properly addresses the reasons resulting into performing the preparation and extraction phase (collection and examination). Through careful analysis, the information is transformed into evidence and the data obtained from the analysis phase is transferred into actions by the use of information obtained during the process in anyway during reporting. For example, the information can be useful in prosecuting some persons involved, it can also be helpful in ameliorating certain activities, or can as well provide supporting-knowledge required to generate new leads in a specified case [122].

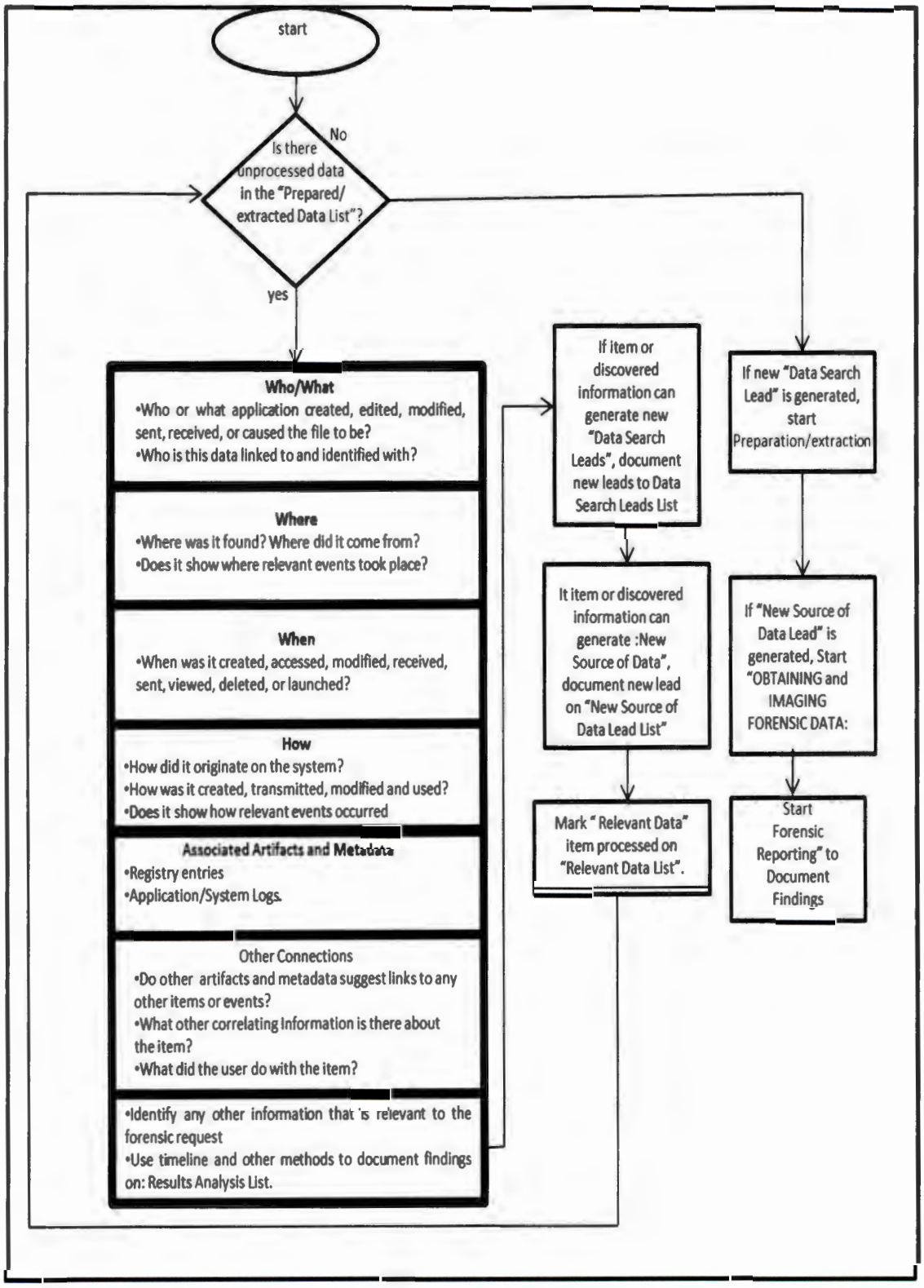

Figure 3.4: Analysis Phase

In the analysis phase, the examiner or analyst ensures that a complete picture for the requester. He/she also ensures that the entire extracted item on the Relevant Data List is examined and all the questions such as: who, what, when, where and how are addressed.

Analysis is the final stage involving the documentation of the results or findings which may involve a detailed description of the actions carried out, specifying other possible actions that should be performed, providing recommendations on how the guidelines, policies, tools and procedures may be improved, including some support on other forensic process aspects. It is one of the main aspects of this study. Once there is no more unprocessed data in the 'prepared/ extracted list' the questions such as who and what should be addressed. The process of analysis tends to provide answers to the question, who, what, where, when, and how? Once it is concluded that there is unprocessed data in the prepared and extracted data list, then the forensic analysis process can commence. However, analysis phase must provide answers to the specific questions which include:

i. Who/What?

In the process of analysis of the identified relevant data it provides answers to the question: what application was created, edited, modified, sent, received, or caused the file to be, who is the file linked to and identified with?

ii. Where?

More so, the analysis process tends to provide answers to questions such as where was the data found? And where did it come from? Does the data show where relevant events took place?

iii. When?

The next question it tries to answer is when was the data created, accessed, modified, received, sent, viewed, deleted, or launched?

iv. How?

In addition, the analysis phase provides answers to the question of how the data originated on the system or network. How was it created, transmitted, modified, and used? And also, does it show how the relevant events or incidents occurred.

Categorically, among other responsibilities of the analyst at this summative and critical stage is to provide answers to these principal questions, who/what, where, when, and how? Furthermore, the analyst or forensic expert also analyses the registry entries and the application/system logs as earlier stated. It also checks other connections for other suggested

useful links and correlating information with what the system or network user did with the data. If any other data of interest are identified, then the analyst may use a timeline or any other documentation method to document the findings in the result analyst list including all the steps taken to reach a conclusion. The Figure 3.4 above shows that, analysis is a continuous process because whenever any new source of data list is identified it re-starts the obtaining and imaging forensic data phase [115].

Generally, having immediately extracted the relevant information, the forensic expert should examine the data so as to obtain reasonable conclusions on the case for documentation and reporting. This phase of the methodology helps the examiner in identifying persons, locations, items, and incidents, as well as determining how those elements are related to each other so as to arrive at the appropriate conclusion. At this stage, documentation is required for presentation to any court of law or the organizations or company's internal actions [115].

3.3.5 Documentation Phase

The next stage after the analysis is the documentation. Documentation is used to keep a comprehensive log of each and every step taken in the data collection and detailed information of all the tools involved in the process. The essence of this is to enable other examiners and analysts to repeat or review the entire process if need be. All evidences that were photographed during the process are also provided here. All the outcomes of the analysis phase are detailed here in the analysis results list. All the information that provided any answer to the analysis-specified questions is also provided here. This is the end of the forensic process before the law enforcement agencies are acquainted with the results. Therefore, it is expected that all newly generated data search leads are collected and processed up to the examination stage and then all the information obtained is documented properly before it is reported [115].

3.3.6 Reporting Stage

The final phase which is involved in the process of preparation and presentation of information acquired/obtained from the analysis phase is the reporting stage.

Finally, after examiners/ analysts go through various phases for quite a number of times and having been able to gather enough information, then they can adequately respond to all the forensic requests. This now gets to the Forensic Reporting phase. At this Reporting stage the examiners/analysts document their findings in such a format that it is understandable to those

who requested for it and they can also be able to apply it depending the case. Forensic reporting is too important to be side-lined, because this is where the examiners/analysts communicate their final findings to the body who requested for the forensic investigation. The significance of the concluded forensic process dwells in the capabilities of the examiners/analysts to communicate the result to those who requested for the forensic investigation [115].

3.3.7 Case Level analysis

The significance of case level analysis is to identify any problem that requires a remedy during the reporting process. At the end of the reporting phase, the requester performs a case level analysis in which he or she together with the examiners will interpret the findings within the context of the entire case. Several factors are possible to affect a reporting process. Those factors include alternative explanation or more plausible explanations. Both must be given considerations. All explanations must be supported using systematic approach.

3.3.7.1 Recommendations

Furthermore, in response to case level analysis, the key recommendations should be pointed out and presented after the analysis in the forensic process.

However, our designed model and its corresponding framework provide the various steps that should be strictly followed in a real time forensic investigation process. But due to the constraints encountered in the demo version of the forensic tool deployed in this research study some of the phases were not practically reported.

3.3.7.2 More Recommendations

i. Furthermore, in response to case level analysis, the key recommendations should be pointed out and presented after the analysis in the forensic process. The recommendations will include: Organizations should perform forensic operations using a consistent process. This guide presents a four-phase forensic process with collection, examination, analysis, and reporting stages. The exact details of each phase may vary based on the need for the forensics.

ii. Analysts should be aware of the range of possible data sources. Analysts should be able to survey a physical area and recognize possible sources of data. Analysts should

also think of the possible data sources located elsewhere within an organization and outside the organization.

iii. Analysts should be prepared to use alternate data sources if it is not feasible to collect data from a primary source.

iv. Organizations should be proactive in collecting useful data. Configuring auditing on OSs, implementing centralized logging, performing regular system backups, and using security monitoring controls will generate sources of data for future forensic efforts.

v. Analysts should perform data collection using a standard process. The recommended steps in this process are identifying sources of data, developing a plan to acquire the data, acquiring the data, and verifying the integrity of the data. The plan should prioritize the data sources, establishing the order in which the data should be acquired based on the likely value of the data, the volatility of the data, and the amount of effort required. Before data collection begins, a decision should be made by the analysts or management regarding the need to collect and preserve evidence in a manner that supports its use in future legal or internal disciplinary proceedings. In such situations, a clearly defined chain of custody should be followed to avoid allegations of mishandling or tampering of evidence. If it is unclear whether or not evidence needs to be preserved, by default it generally should be preserved.

vi. Analysts should use a methodical approach of studying the data. The foundation of forensics is using a methodical approach in analysing the available data so that analysts can either draw the appropriate conclusions based on the available data or determine that no conclusion can yet be drawn. If evidence might be needed for legal or internal disciplinary actions, analysts should carefully document the findings and all steps taken.

vii. Analysts should review their processes and practices. Reviews of current and recent forensic actions can help identify policy shortcomings, procedural errors, and other issues that might need to be remedied, as well as ensuring that the organization stays current with trends in technology and changes in law [115].

Consequently, having described the general principles of the digital forensic analysis process, it is important to relate the relevant data to be considered to be the fingerprint biometric. This study emphasised that biometric characteristics such as fingerprints can enable digital forensic investigation and analysis. This implies that when biometrics is involved in a crime

scene it follows the same process/methodology until a conclusion is reached. Therefore, presented below is the collection and analysis of fingerprints in the physical environment.

3.4 Automated Digital Forensic Process

The digital forensic process is evolving from the conventional manual methods to a variety of automated tools that are commonly used today. Forensic examiners could perform several analyses using the manual process. However, as technology became more sophisticated, forensic examinations have evolved at the same pace with the technology. This evolution to automated tools happened when software developers began creating an assortment of automated tools to interpret data and perform the forensic examination. Today's automated tools are often a more efficient method for forensic examiners to collect and analyse digital evidence which gain the same results. Depending on the situation and the type of device and media, different forensic methodologies are used. Standards and Best Practices require examiners to perform analysis from a bit-by-bit copy of the original data to ensure data/feature integrity. This bit-by-bit copy is commonly referred to as a forensic image. Depending on the circumstances an examiner is confronted with, forensic analysis can be performed at the logical or physical level of the device or media. Traditional command-line techniques and automated tools each have their own purposes during forensic examinations. Time constraints, the type of examination, and exigent circumstances are some examples of why a particular methodology might be more appropriate to use during an examination over another operation [116].

However, some among the forensic community are busy considering implementing future technologies for more automation in forensic science due to the rate of adaptation of the current technologies and the effective utilization of forensic products by customers. Moreover, automation in forensic science is on the increase as strong tactical approaches are developed in defining the forensic products of the future. Additionally, research is on-going, in designing long-term strategic plans [113].

Thus, the automated tools that are available to law enforcement and forensic examiners can be divided into three main groups such as imaging tools, triage tools, and analysis tools. A few of the most popular automated forensic tools used by law enforcement forensic labs nowadays include: WinHe, EnCase, Access Data Forensic Toolkit, Advanced PDF Password Recovery and various Linux tools. However, the availability of these tools relies on the budgets of the agencies: Commercial Forensics [117, 118, 119]. Also, automated tools are

being developed to carry out several forensic functions such as live system acquisition and small-scale device interrogation. These tools are regularly updated and new tools are also being developed due to the ever-changing varieties of computer systems. The computer systems range from cell phones, and several other portable or hand-held digital devices as well as the deployment of other forms of identity authentication such as fingerprint biometric.

Apparently, forensic tools perform several functions and operations like data recovery; disk imaging; integrity checking; password recovery; remote access; sorting; permanent file deletion; Searching, and, they are quickly replacing the human or manual forensic expert examination [120]. Here we performed data recovery by discovering the password to decrypt an encrypted PDF document using the Advanced PDF Password Recovery Tool. The essence of this is to indicate the viability and usability of the forensic software packages.

3.5 The Advanced PDF Password Recovery Window

This window displays the several functionalities of the software which enable the recovery process. The attack under investigation is a brute force attack. This attack in cryptography is a cryptanalytic attack that is used against encrypted data [121]. This type of attack is used when it is impossible to take advantage of other weaknesses within an encrypted system. However, the Advanced PDF Password Recovery tool decodes data that are encrypted passwords or Data Encryption Standard (DES) keys, through determined effort like employing the brute force. In the window below, we identified the type of attack to crack the password protected portable document format (PDF) file.

Also the required options are selected from the Brute force range of options.

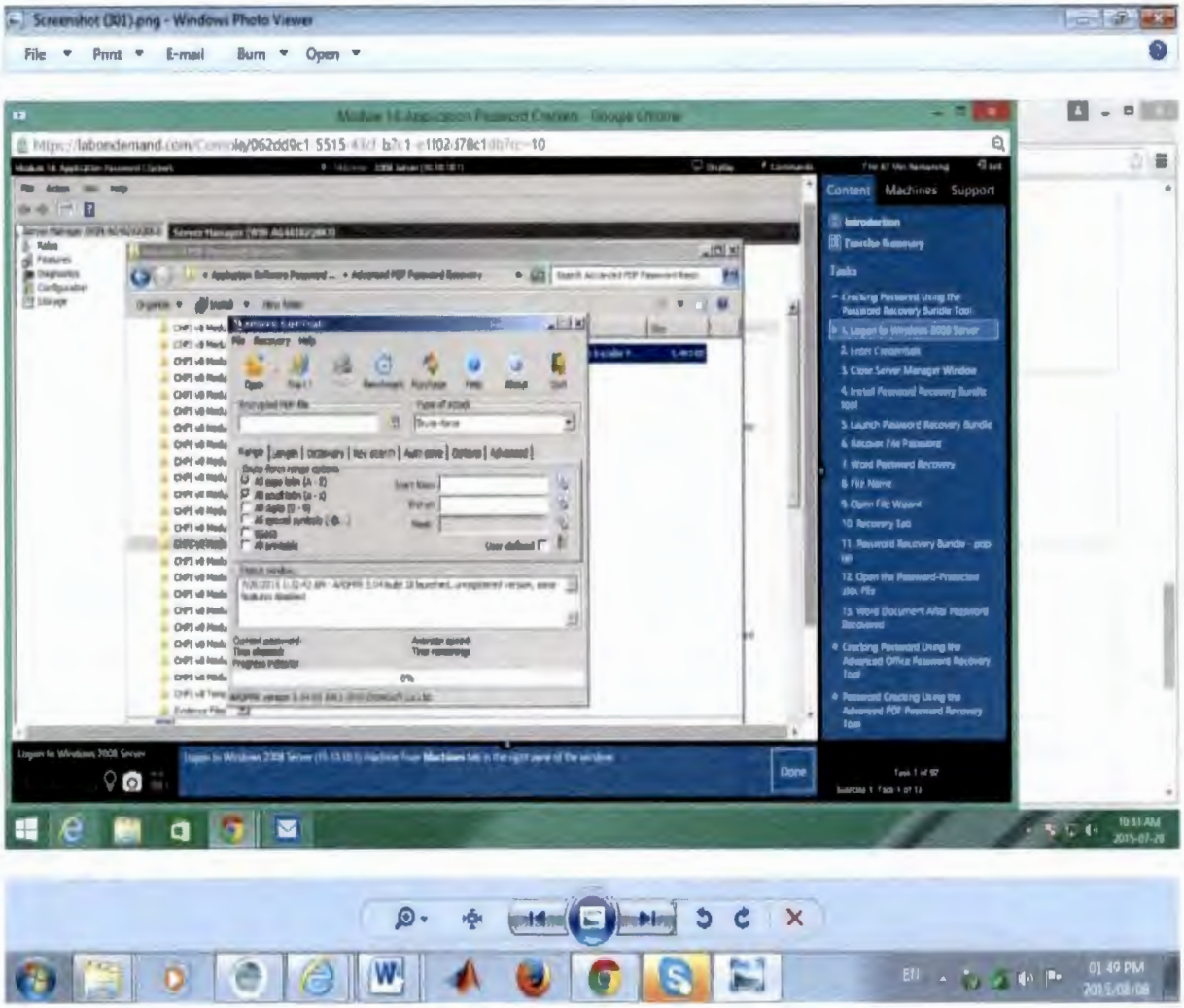

Figure 3.5: Advanced PDF Password Recovery main window.

Also indicated in the Figure 3.6 below, is "the any password option from the advanced tab. This enables the search range for the password of the encrypted PDF files.

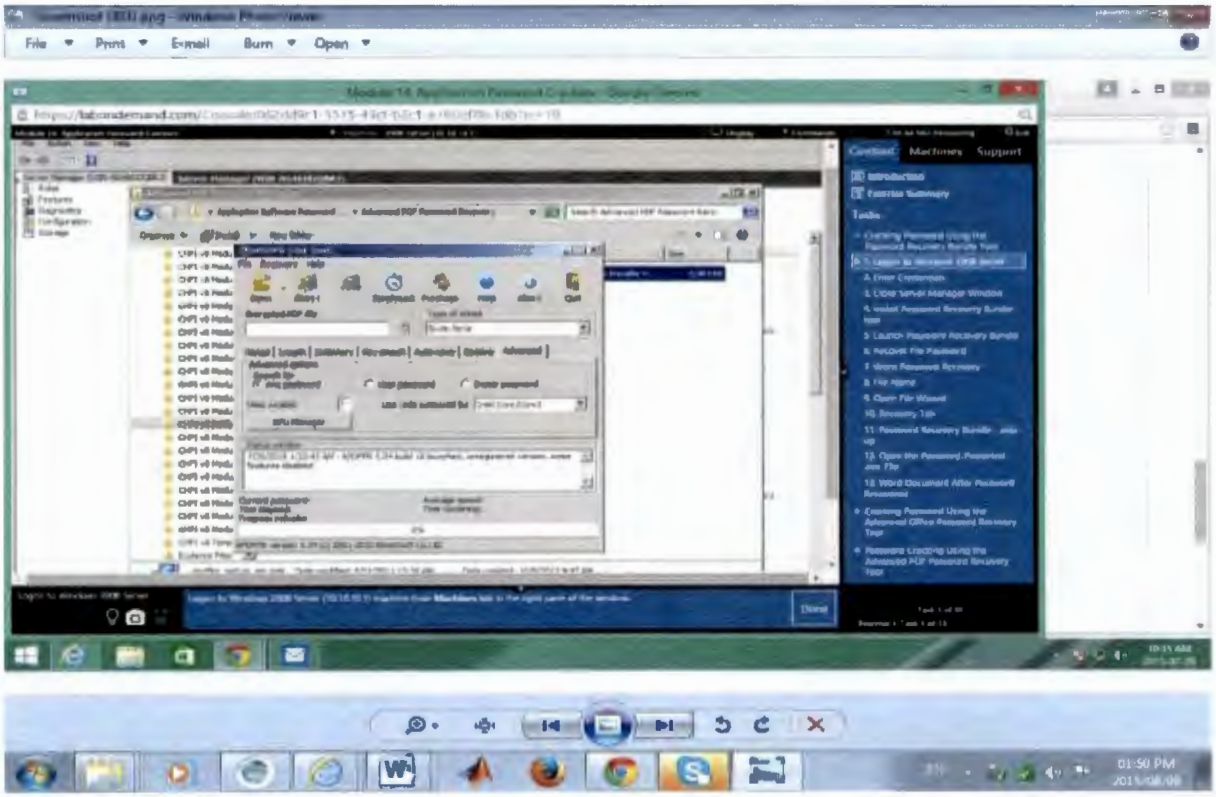

Figure 3.6: Selecting type of Attack and range of options

From the open tab in the Figure3.7 below, browse for the password protected PDF files and selected the encrypted file among the PFD file discovered as shown in the figure below.

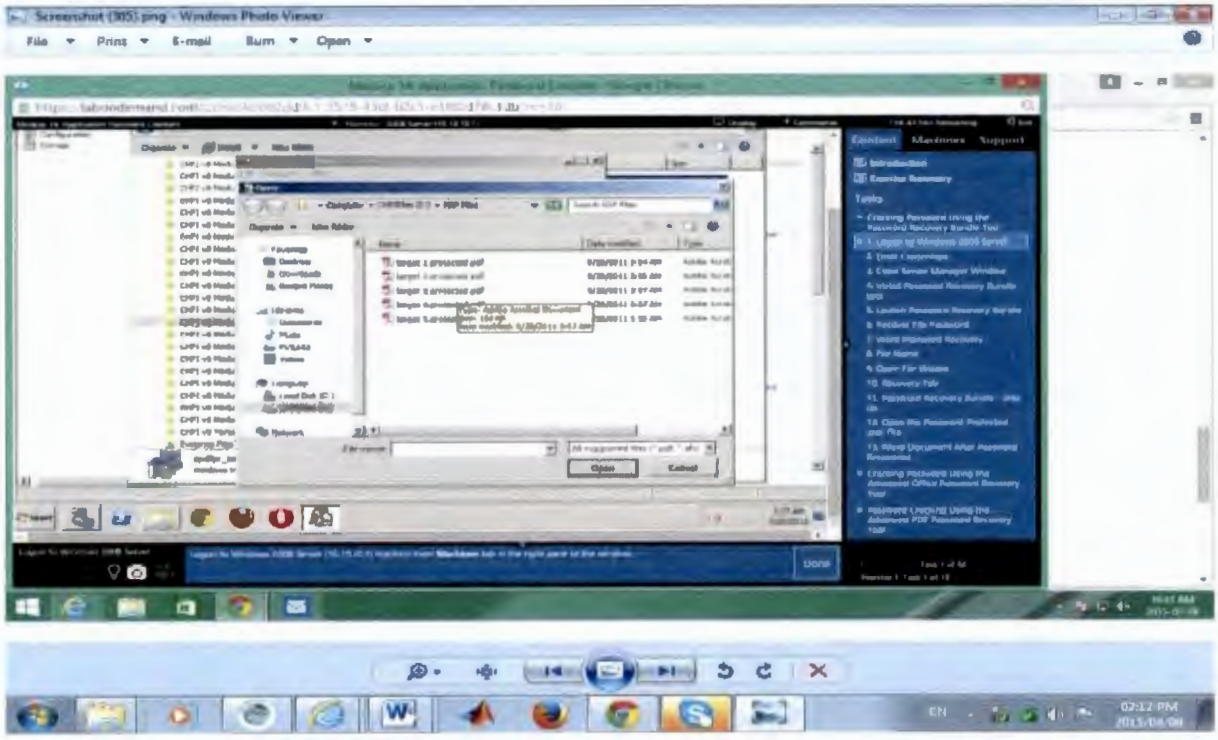

Figure 3.7: Selecting a password protected PDF file

Indicated in the Figure 3.8 below is the start recovery window which shows the recovery process of the password for the encrypted file.

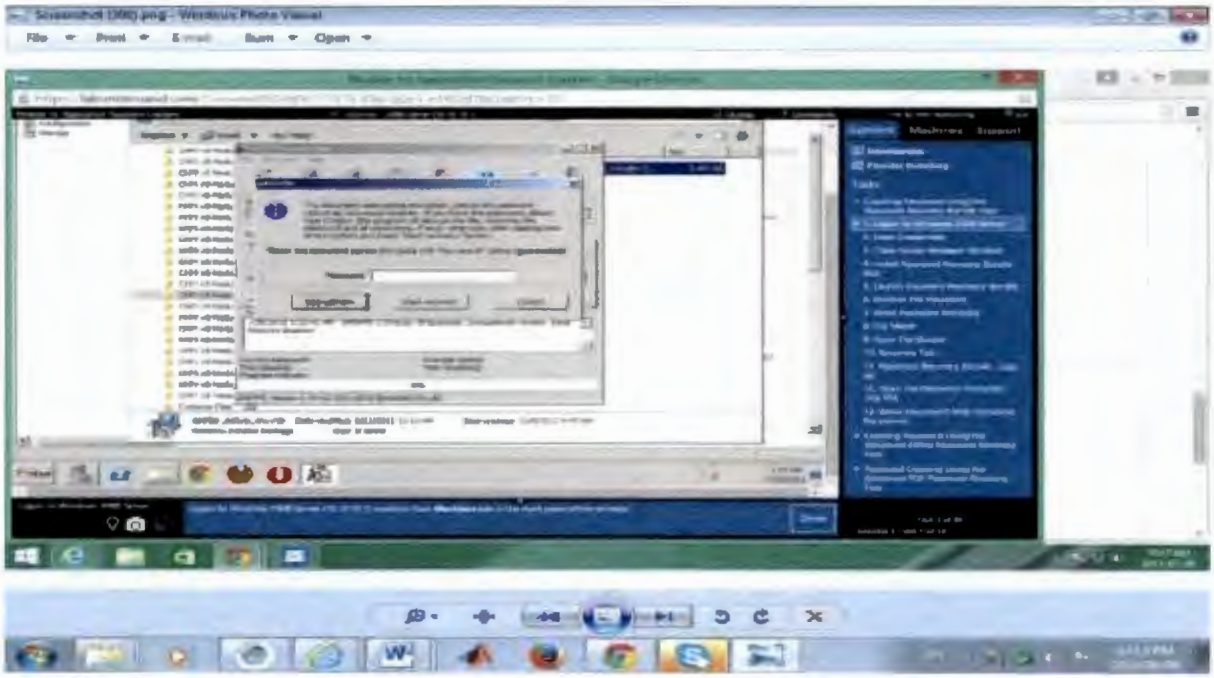

Figure 3.8: Selecting Password Recovery Process

Indicated in the Figure 3.9 below is the successful recovery of the password for the encrypted file. This resulted into the successful decryption and recovery of the PDF file presented in subsequent figure 3.10 below.

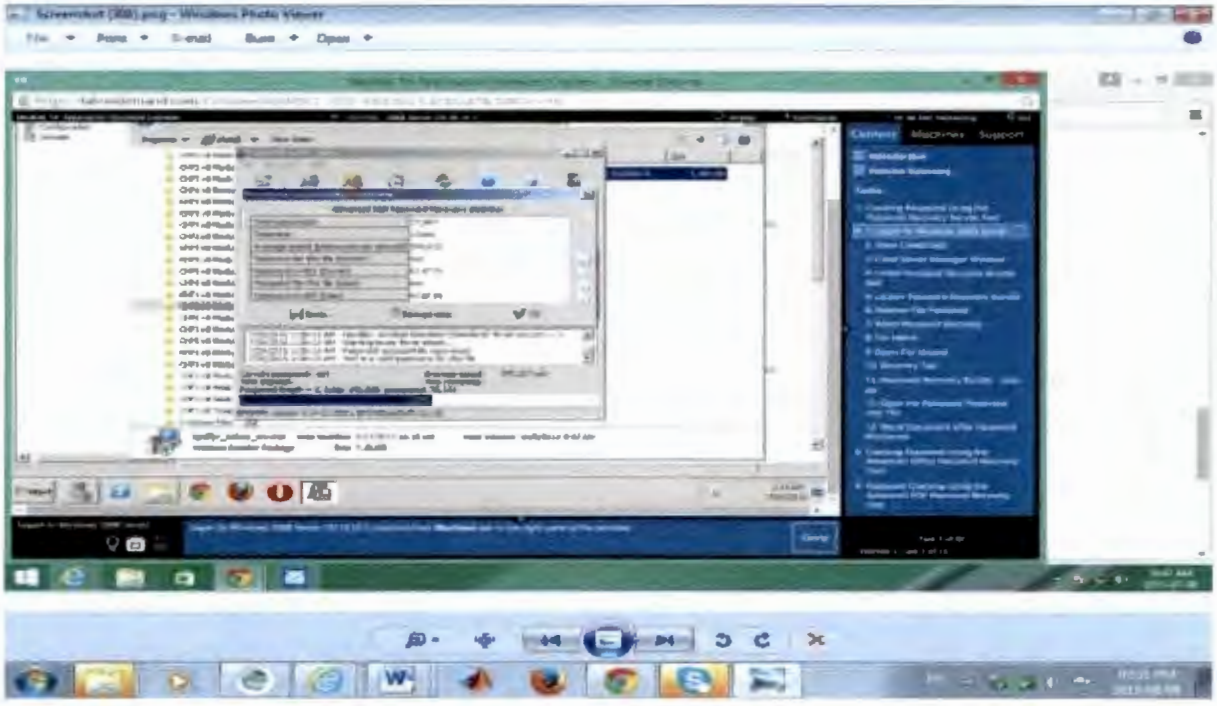

Figure 3.9: Displaying cracked Password of PDF file

From the Figure 3.10, it is evident that the successful deployment of forensic science software provides adequate solutions to information system security and network management.

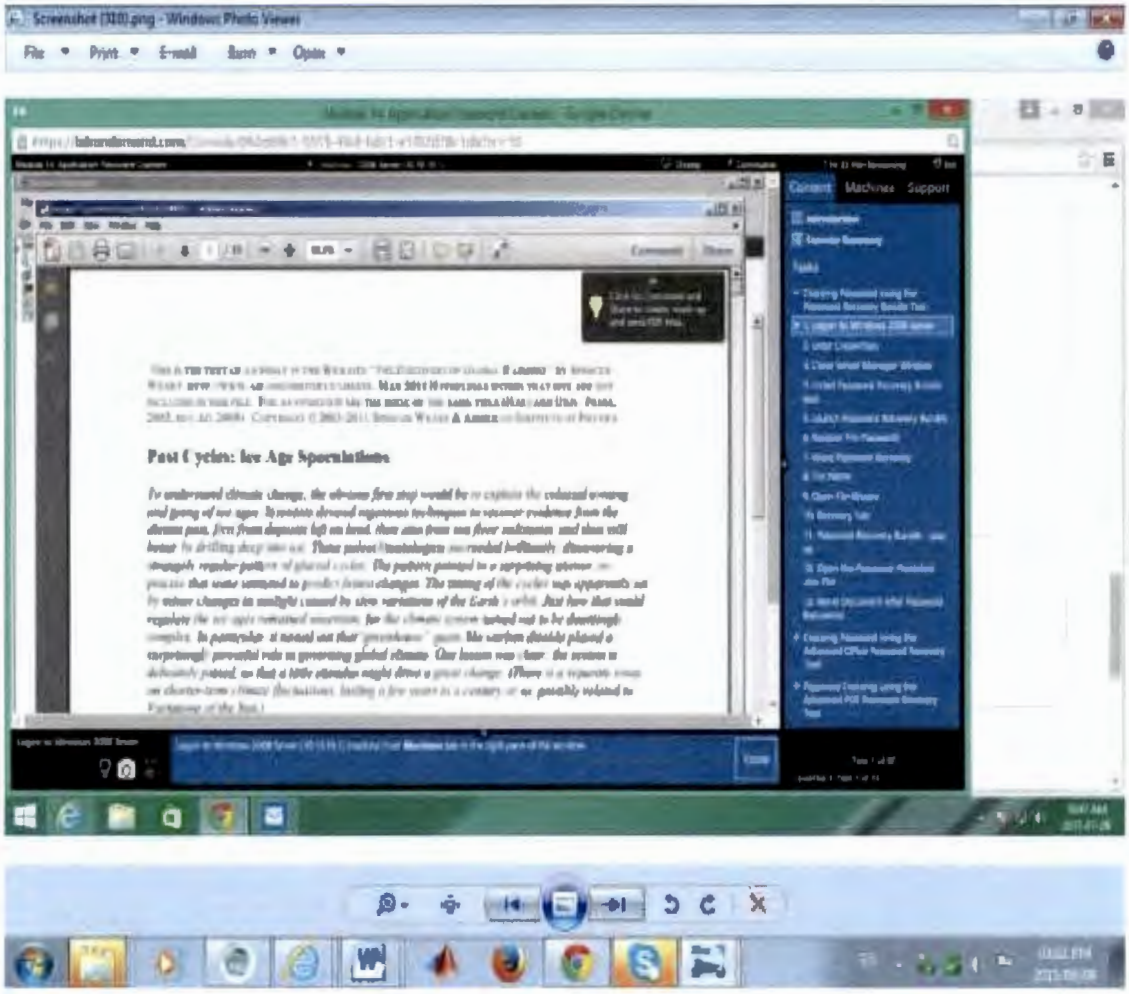

Figure 3.10: Displaying the Decrypted PDF file

Aside the computer forensic investigations, when fingerprints are involved in crime screen they can as well be investigated and analysed for the right prosecution. The details are described below.

3.6 Automated Fingerprint Forensic Analysis Process

Any fingerprint involved in a crime scene goes through a process which involves location, collection, and examination in order to identify whether or not a particular fingerprint is involved in a crime. Locating and collection of fingerprints at crime scene can be manually or automatically performed. Fingerprint analysts or examiners usually use the analysis,

comparisons, evaluation and verification (ACEV) process in order to determine each fingerprint [122, 123]. Each component of the process is discussed below.

i. **Analysis:** At this stage the fingerprint is thoroughly accessed to determine if it is suitable for a comparison. If the fingerprint cannot be used for comparison due to inadequate quality or quantity of features, then the examiner ends the examination and the fingerprint is discarded and reported as not suitable. If the fingerprint is suitable, the analysis will specify the features to be used in the comparison and the degree of variations that will be accepted. However, the analysis may also disclose the physical features such as curves, deltas, creases and scars that can help to indicate where the comparison is expected to begin. More details of the analysis stage are reported in section 3.3.4 above.

ii. **Comparisons**: At this stage the analyst performs the comparison by viewing the known and the suspect fingerprints on both sides. The analyst then compares the minutiae characteristics and locations to determine if they match (if they are similar). Known fingerprints are usually collected from persons of interest which includes: victims, persons present at the crime scene or through a search of one or more fingerprint databases which includes automatically performed the automatically performed Integrated Automated Fingerprint Identification System (IAFIS). The FBI IAFIS is the largest fingerprint database in the world. As at June 2012, research shows that it contained over 72 million fingerprint records both from criminals, military personnel, government employees and several civilian employees. This comparison is mathematically reported in section 4.2 and 4.2.1.

iii. **Evaluation:** At this stage the examiner solely and ultimately decides if the prints are from the same person/source (identification or individualization), if they are from different persons/sources (exclusion) or it is inconclusive. The inconclusive output may be as a result samples of too poor a quality, lack of comparable areas, or insufficient number of similar or dissimilar features to conclude. The significance of evaluation is to make a decision or draw a conclusion. This is the decision threshold which is determined by the examiner or the analyst as the case maybe.

iv. **Verification**: At this stage another examiner can be allowed to independently analyse, compare and evaluate the fingerprints in order to support or disprove the conclusions of the original or former examiner. At this level the examiner may also verify the

correctness of the establishments reached in the analysis phase. The essence of verification is to validate the earlier decision or judgement over a case.

3.7 Manual Fingerprinting Forensic Process

Any fingerprint evidence left behind by the suspects or victims can be used to identify who was at a crime scene and what the person touched. Hence, it is necessary for defence attorneys to know, and as well inform the jury, that the tool/techniques used to locate, collect and identify fingerprints are far from a perfect science. An understanding of how fingerprints are located and collected can help the attorneys to identify if a flawed analysis was performed by investigators/ analysts or lab technicians. More so, more knowledge of the various fingerprint collection techniques is essential to successfully cross-examine the crime scan information as presented by the technicians and fingerprint examiners. This presentation then attempts to provide an overview of the tools/ techniques used to locate, collect, and identify a fingerprint [124,125,126]

3.7.1 Major Fingerprint Collection Methods

In this section various collection methods for fingerprints involved in a crime scene are discussed.

Step1: Locating the fingerprints

Locating of fingerprints often demands a careful and calculated search. However, in physical circumstances where the fingerprint is visible, it is relatively easy to locate/find a fingerprint. Alternatively a more intricate search is required when the fingerprint on any surface is not visible. The amount of time and effort required to investigate and analyse a fingerprint is determined by the type of fingerprint that is left behind. There are basically three types of fingerprints according to Forensic Science [127, 128]. These are a patent print, a plastic print and a latent finger print.

A. Patent Fingerprints: These types of prints are easy to find because they are visible to the naked eye. Patent prints are left particularly when someone has a substance on their fingers such as grease, paint, blood, or ink and touches a surface.
B. Plastic Fingerprints: Plastic prints are less common compared to the patent prints but they are very easy to pick up. They are a three-dimensional impression of the finger left behind on an object when someone touches an object such as wax, butter, or soap.

C. Latent Fingerprints: This type of fingerprints is the most common type and they take the most time and effort to find because they are invisible. When someone touches any porous or nonporous surface the latent prints are left behind. The natural oils and residue on fingers leave a deposit on surfaces which mirror the ridges and furrows that are present on the individual's finger [129, 130, 131].

Categorically, investigators and analysts often embark on a two-phase process when looking for fingerprints.

I. First phase: This includes looking for patent and plastic prints since they are visible. A flash light is used most times during this phase.
II. Second phase: This includes a blind search for latent prints. In Order to make the search thorough, investigators usually focus on the entry and exit points that the suspect might have used and any other objects that appear to have been displaced, which includes; overturned lamps or possible weapons. However, the type of surfaces that are being searched for fingerprints are often determined by the techniques/tools the investigators/analysts employed to search for the fingerprints [129, 130].

3.7.2 Nonporous Surfaces

A powder technique is often used to identify latent prints on nonporous surfaces such as glass, marble, metal, plastic and finished wood. Once the powder is spread on the surface, it adheres to the residue deposited from the finger's touch; this enables the investigators to locate the print. The print is used often times to avoid smudging, a magnetic powder technique is also used on the print in which the powder is poured on the surface and then spread evenly over the surface using a magnetic force instead of spreading the powder with a brush. This makes the colour of the powder to contrast with the surface that is being searched to in order to allow better visibility. For instance, the investigator/analysts should be able to use a white or grey powder if searching a black marble countertop for prints .Moreover; it is the duty of the attorneys to inquire if the crime scene technician who collected prints using fingerprint powder used a disposable brush. When a brush is reused in different locations at a crime scene or reused at another crime scene, the brush can transfer trace amounts of DNA evidence.

Superglue fuming is another popular technique for fingerprint location and identification which is used by both lab technicians and investigators at the crime scene. This is a chemical

process that exposes and fixes fingerprints on a nonporous surface. An airtight tank in the lab known as a fuming chamber, releases gases that adhere to the oily residue of print, which in turn creates an image of the fingerprint. This technique-Superglue fuming can also be performed at the crime scene. Instead of using a fuming chamber the crime scene investigators may use a handheld wand that heats up superglue and a florescent dye. However, performing the Superglue fuming at the crime scene can be relevant in preserving prints on items that are being sent to the lab through mail. One of the disadvantages of this act is that if the evidence is fumed for a very long time, it can distort the print, and render it useless [129, 130].

3.7.3 Porous Surfaces

When it comes to porous surfaces such as fabric, unfinished wood, and paper, the powder technique is not very effective. Therefore, investigators often use chemical methods to locate the print which includes iodine fuming, *silver nitrate, or ninhydrin.* When one of these chemicals comes into contact with the chemicals present in the fingerprint residue (natural oils, fats), the print become visual. The *Ninhydrin* has the ability to react with specific components of the latent fingerprints residue, which include amino acids, and inorganic salts. The chemical reacts on fingerprints by making them change to a purple colour. Once it turns purple, it can quickly be photocopied.

In iodine fuming, a fuming chamber is used. The process works by heating up solid crystal iodine which creates vapour that adheres to the oily residue of print. This produces a brown coloured print. One of the challenges of using iodine fuming is that the print fades quickly once the fuming has taken place and therefore it must be photographed quickly in Order not to lose it. .If the print is sprayed with a starch and water solution it can be preserved for several weeks.

Also, when silver nitrate is exposed to latent prints it reacts with the chloride of the salt molecules found in fingerprint residue which forms silver chloride. When exposed to ultraviolet light, silver chloride turns black or brown, making the print visible. Particularly, this method works better on impressions left in cardboard and paper-like surfaces

Similarly, *Ninhydrin* is often commonly used than iodine fuming and silver nitrate techniques to find a latent fingerprint. The object on which the fingerprint resided can be dropped in or covered with a *ninhydrin* solution by spreading. It then reacts with the oils in the fingerprint's

residue which create a bluish print. One of the disadvantages of using *ninhydrin* is its very slow reaction. It often takes several hours for the fingerprint to become visible. In order to increase the reaction, the object which contains the fingerprint can be heated up to 80 to 100 degrees or the use of hot iron on the specified paper. Several other techniques are available which are sometimes used. For instance, laser illumination which creates a contrast between the print and the surface also exposes the print [126, 127, 128, 129, 130, 131].

3.7.4 Human Skin

It can be incredibly difficult to locate and identify fingerprints which are left on human skin. The initial major challenge is to locate the fingerprint because the oily residues that are left by the fingerprint itself are deposited (present) on the top of human skin. This makes it difficult to differentiate between the skin surface and the print. More so, once the fingerprint is left on the human skin, the oily residue disappears, and gets absorbed into the skin, and this makes the fingerprint blurred. For this reason fingerprints left on human skin do not stay available for a long time. The duration at which it can last is maximum of 2hrs. However, there are special techniques for capturing prints from skin, clothing and other difficult surfaces. Amido Black, a technique used in capturing fingerprints deposited on the skin and other difficult surfaces. It is a non-specific protein stain which reacts with any protein present. It is suitably used in developing or enhancing impressions of blood on human skin. Additionally, in order to reveal fingerprints on clothing, high-tech methods which include the vacuum metal deposition that makes use of gold and zinc are more promising for forensic examiners and analysts [126, 127, 128, 129, 131].

3.7.5 Textured Surface

Textured surfaces include all non-smooth surfaces (rough surfaces) like painting and other rough strokes or scares balls. They make the identification and collection process of fingerprints even more difficult but never impossible. However, *AccuTrans,* is a liquid casting compound which is used in lifting powdered latent prints from rough, textured or curved surfaces. Basically, *AccuTrans* is a very thick liquid which fills in the nooks and crannies of rough or textured areas where other methods finds it difficult to acquire results.

Step 2: Photocopying the Fingerprint

It is very important to photocopy the fingerprints once located before they are lifted. This is because photocopying captures even the location of the fingerprint on other objects as well as

the orientation of the fingerprint, then the photograph can be a relevant data sources, a major source of identification of information Patents or plastic print and it can then be used comparing and matching of the fingerprint to its original source. Taking the photographs of the fingerprints at once at the same crime scene really helps to avoid the tampering of evidence and supports evidence integrity [125, 126, 127, 128, 129, 130].

Step 3: Lifting the Fingerprint

This means making a permanent impression of fingerprint. This is possible on flat round surface. A rubber tape is used in lifting a fingerprint with adhesive surface that is usually applied on the fingerprint. This automatically leaves an imprint on the tape. Most times a ruler can be used to swipe across the top of the tape slowly to make sure no rubber or object is on top of the tape when the tape is peeled off from the surface, then a plastic cover is placed on the adhesive in order to prevent disruption or tampering of the print. Next is to place identification information on it including a description of the location and sources of the fingerprint. After lifting the fingerprint it is then converted into digital data and moved in order to create a clearer image [134, 135, 36, 137, 138, 139].

3.7.6 Other Fingerprint Collection Methods

Here we discuss other methods apart from the major methods we described earlier, several other methods can as well be used which includes: Dusting, Alternate light source (ALS), Cyanoacrylate, and Chemical Developers [125, 126, 127, 128, 129, 130].

i. **Dusting:** This involves dusting a smooth or non-porous surface with a black granular or aluminium plate, black magnetic powder, and when the fingerprints appears they are photographed and preserved from tampering, then the clearer adhesive tape can be applied for lifting. This is not very reliable as the tape for lifting and the powder have the possibility of contaminating the evidence; therefore the investigators and examiners should be very careful to perform other evidence extraction and other techniques, to boast the reliability of the result.
ii. **Alternate light source (ALS):** The use of this method is increasing as investigation now is to examine any likely surface with doors, doorknobs, windows, railings etc. This is a LED device that emits a particular wavelength, or spectrum of light. Some of these devices make use of different filters in order to provide varieties of spectra which are used to also photograph or process further with powder or dye stains.

Sometimes investigators also use blue light that has orange filters to filter and locate latent prints that are on desks, chairs, computer equipment or other objects at a crime scene. Use of various alternate light sources may help enhance the appearance of a fingerprint.

iii. **Cyanoacrylate:** Investigators usually perform cyanoacrylate (superglue) processing; they can also fume on the surface before applying the powdering method or dye stain method. When performing this process on non-porous surface, it involves the exposure of object under examination to vapours. The vapour (fumes) will comply with any prints that are present on that object by making them visible with oblique ambient light or shows a chamber that is specifically design to expose latent prints to superglue fumes. It has been verified that super glue fumes comply with latent fingerprints on the neck of a glass bottle.

iv. **Chemical Developers:** Another chemical used to locate latent fingerprints on porous surfaces is DFO (1, 2-diazafluoren-9-one); it makes fingerprints to fluoresce, or glow, when they are illuminated by blue-green light. Paper treated with *ninhydrin* reagent can also reveal latent prints after being processed with a household steam iron. Moreover, like fingerprint powders, chemical processing can reduce the investigator's ability to perform other techniques that could reveal valuable information. For example, a ransom or holdup note will be examined by a documents expert before being treated with *ninhydrin* because some formulations of *ninhydrin* will cause certain inks to run thereby destroying the writings on it. Therefore, any non-destructive investigations are performed quickly before the evidence is treated with chemicals in order not to lose it.

Step 4: Comparing Fingerprints

The final step includes a very close examination and analysis of the characteristics of the fingerprints. In fingerprints digital forensic examination process utilizes the ACE-V process explained earlier in section 3.6 above. This method compares a fingerprint that is collected from any crime scene to a set of known fingerprints already stored in a database. This also corresponds to our initial description of minutiae matching method. Fingerprint analysis is conducted by forensic scientists/analysts, technicians or police officers, law enforcement agencies or crime laboratories. However, the analysts / examiner should have the proper training and experience to perform the task. Currently many agencies require new examiners to have a four-year degree in science (Computer Science, biology, chemistry or physics). In

addition, agencies may require analysts/examiners to become certified by the International Association for Identification (IAI). More so, in criminal justice cases, computerized systems are used to search various local, state and national fingerprint databases for potential matches. Many of these systems provide a value indicating how close the match is, based on the method used to perform the search. Fingerprint analysts or examiners then review the potential matches and make a final determination. However, casework can also be sent to private companies if there is a need, such as to reduce backlogs, verify results, or handle high-profile cases [125, 126, 127].

Moreover, in manual fingerprint forensic processes the fingerprint is extensively observed based on the quality and quantity of information in order to find agreement or disagreement between the unknown fingerprints (from the crime scene) and known prints stored in the database. In conducting the examination, fingerprint examiners/analysts use a small magnifier called a loupe to view minute details (minutiae) of a print. Usually, a pointer which is called a ridge counter is used to count the friction ridges as shown in the figure below.

Figure 3.11: Viewing Fingerprint Minutiae using a Loupe

Fingerprint forensic process is a comparison or a matching process. It is defined as a means of discovering similarity and dissimilarity among any two given fingerprints images.

Fingerprint comparison can be best seen as taking a paper copy of a collected fingerprint image with its minutiae marked or overlaid and a transparency of a known fingerprint with its minutiae marked or overlaid. Placing the transparency of the known fingerprint over the paper copy of the collected fingerprint, translating and rotating the transparency, one can

locate the minutiae points that are similar in both fingerprints. The examiner considers the number of similar minutiae discovered, their closeness of fit, the quality of the fingerprint images, and any contradiction in the minutiae matching information in other to assess the similarity of the two fingerprints. After this he draws a conclusion which based on the discovery which can transcend into verification by another examiner. Apparently, manual fingerprint forensic process can be a very tedious and cumbersome task. Therefore, the automated fingerprint forensic process is recommended [124, 127, 128].

3.8. Chapter Summary

In this chapter, we reported the Analysis of Digital Forensic Technology by designing Digital Forensic Analysis Model and discussing the phases specified in the model. They include Preparation and Extraction Phase, Examination Phase, Analysis Phase, Documentation Phase, Reporting Phase, Case Level analysis, and Recommendations phases. Also, in this chapter we analysed, the Fingerprint Forensic Analysis Process, Manual Fingerprint Forensic Process, Major Fingerprint Collection Methods, Other Collection Methods and the Automated Fingerprint Forensic Process. The essence of this analysis is to specify the principles of digital forensic technology and establish its relationship with fingerprint biometric technology. The two security systems share the same objective which is to identify impostors and criminals. Biometrics complements forensic analyses in cases that have legal implication.

Chapter 4

Analysis of Biometric Technology

4.1 Chapter Overview

This chapter describes in details the basic operations which are performed on any person's fingerprint in order to determine its uniqueness. We have mentioned earlier that there are no two persons in the world having the same fingerprint. Therefore, in this chapter we discussed the various stages, algorithms and the synthetic fingerprint generating tool SFinGe employed to generate and extract a fingerprint sample in the absence of a fingerprint scanner to be used to obtain a fingerprint. This operation provides an answer to research question 2 and its corresponding objective. It involves generating and extracting the fingerprint minutiae point using the algorithms of fingerprint image processing which raises the security level of biometrics authentication and identification system. These several stages were represented in source codes and implemented in MATLAB software tool. The SFinGe software generated a sample of the fingerprint to get the actual fingerprint which was used in the MATLAB for minutia point extraction. It involves *binarization,* and *thinning.* Fingerprints undergo these stages in other to determine their uniqueness which differentiates the other.

i. Binarization: Binarization requires a binary fingerprint image and the image usually passes through the line thinning process of converting the grey image given out an image where pixels assume a binary image. The binarization performed applies two different elaborations to the input image: an average filter and a thresh operation with two different thresholds.

ii. Thinning: Thinning involves the papillary lines from the previous varying thickness. It ensures that algorithms for minutiae extraction are as simple as possible. It minimizes the ridges thickness to the unitary value.

However, the essence of this in regard to the context of the research work is to indicate the underlying stages of the fingerprint that provides its uniqueness and individuality for effective, efficient and reliable authentication and identification system that promotes digital forensic technology. By this method the actual feature or image (minutiae) of the fingerprint to be used to implement the biometric authentication system is generated for onward implementation of security processes.

4.2 Simulation Setup

In this phase we reported the SFinGe software experimentation. The simulation step begins by opening the SFinGe software main window. In this window we indicated the sensor area, resolution and the area of acquisition to be 0.51x0.67 and we assumed the size of 256x336 pixel image for the master fingerprint to be generated. This process starts by first generating the master fingerprint, it forms the binary image and does not contain both texture and noise core. The process of fingerprint generation begins with creation of the master fingerprint image, which is the binary image that does not contain any texture or noise core. The process comprises of the fingerprint shape, followed by a directional map and then the density map. They are all separately generated.

4.2.1 Fingerprint Mask / Shape

The Figure 4.1 represents the fingerprint mask that was generated when the sensor area is setup. The sensor area is selected and the shape of the fingerprint mask is selected and the region of the finger is also determined which is the global shape of the thumb. From the image below we understand that the system security administrator has the choice of choosing the type of finger he would like to make a sample of. There are several choices an administrator can choose from the index, thumb, medium, ring or little finger. The shape of the finger is determined by the parameters the system security administrator set on fingerprint mask.

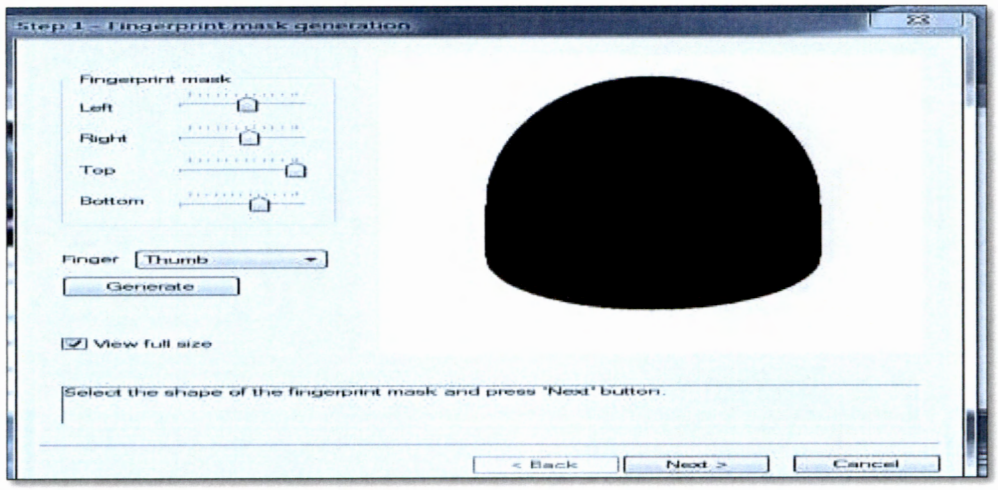

Figure 4.1: Generated Fingerprint Mask

4.2.2 Fingerprint Directional Map

The Figure 4.2 represents the directional map that is generated from the fingerprint mask. Positioning the core and delta appropriately using the left loop fingerprint generates the directional map. The stage system security administrator determines the fingerprint class, and the orientation. Here, the left loop fingerprint class is used.

Figure 4.2: Generating Fingerprint Directional Map

4.2.3 Fingerprint Density Map and Ridge Pattern

In this segment we created the density map and the ridge density based on some secondary criteria from the visual inspection of the master fingerprint. This is determined by adding a little spike in the middle/centre of the fingerprint image and randomly applying several spurious Gabor filters within the white image. Then the orientation of the filter altered in line with the directional and density maps which surfaces the minutia in random points. The Figure 4.3 represents the Fingerprint Density Map and Ridge Pattern generation interface.

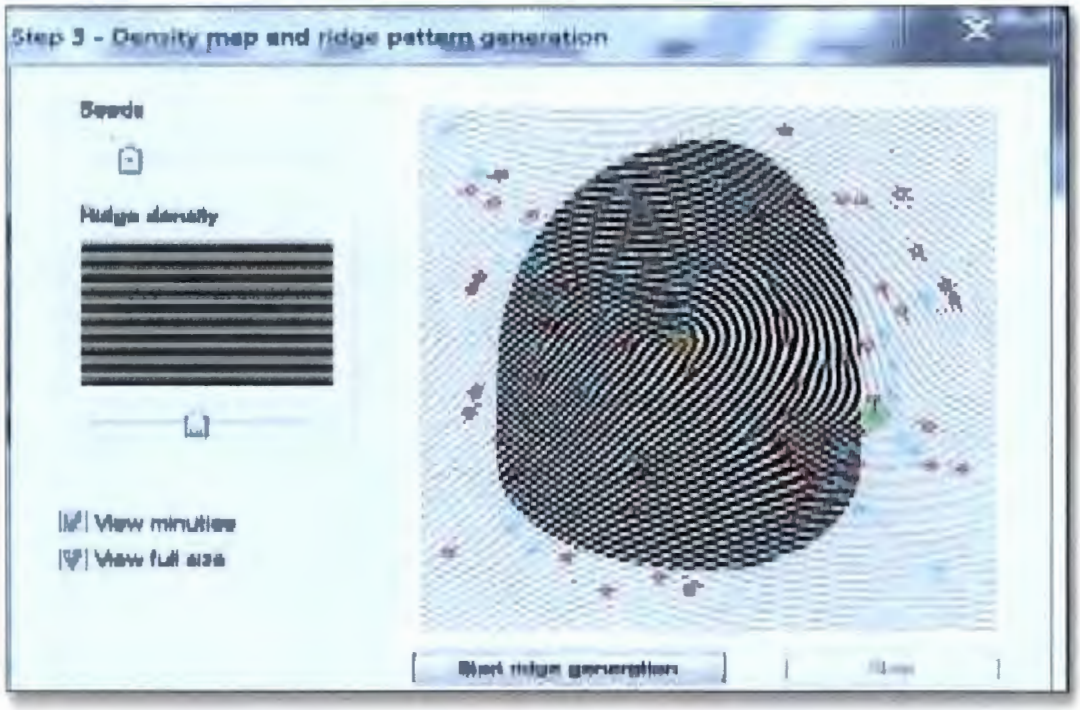

Figure 4.3: Fingerprint Density Map and Ridge Pattern

4.2.4 Fingerprint Permanent Scratches

In this segment, the space variant linear filtering, the orientation and frequency of the filter are locally altered in line with the directional map and the density map in order to determine the permanent scratches on the fingerprint. This is presented in the Figure 4.4 below.

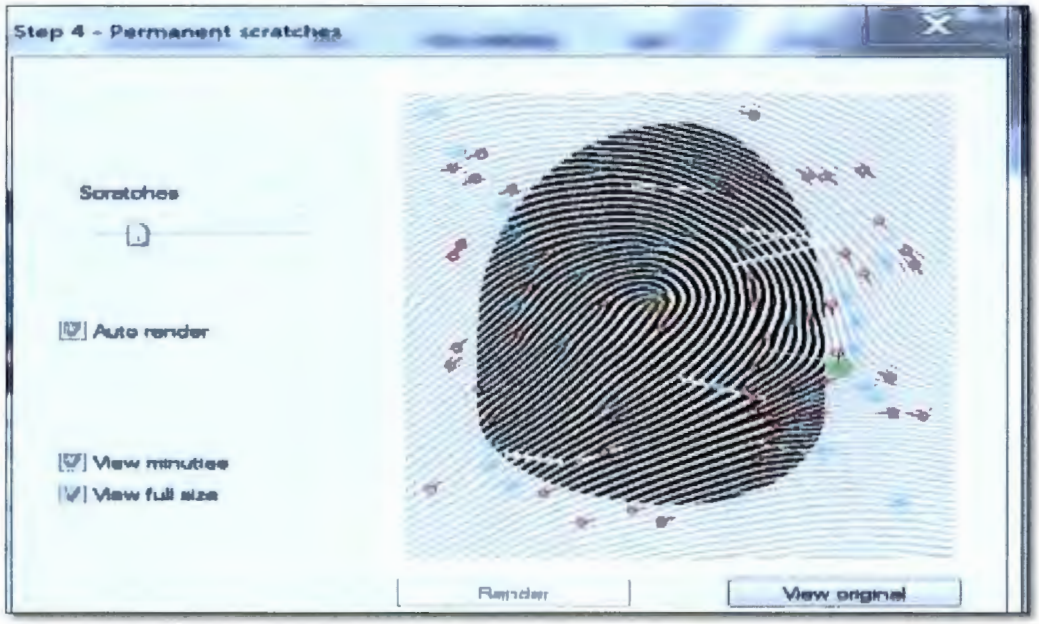

Figure 4.4: Fingerprint Permanent Scratches

The addition of more pressure gives rise to the surface friction that disallows any form of dry skin within the contact region. The position of the contact region is indicated in Figure 4.5 below.

Figure 4.5: Fingerprint Contact Region

The increase in noise is a result of addition of pressure which makes the finger appears drier. Whether oily or wet fingers the prints produced indicate altered ridge flow. The effect of both pressure and dryness is indicated in the figure 4.6.

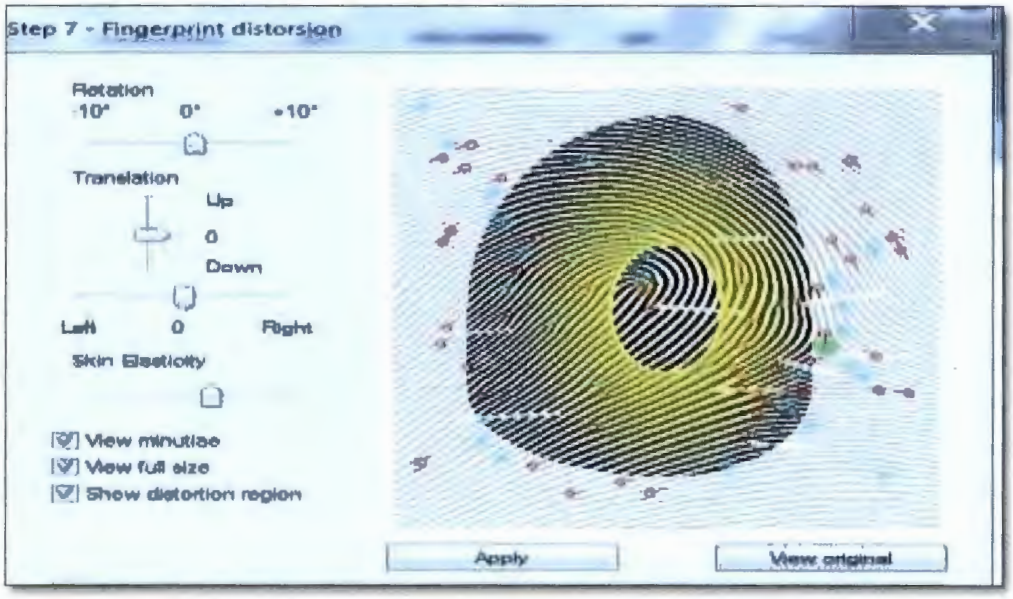

Figure 4.6: Fingerprint Pressure/Dryness

4.2.5 Fingerprint Image Distortion

When a fingerprint is positioned on the surface of the sensor/scanner, torsion and traction forces may be applied on it which results in possible distortion. At this point all the pixels are remapped in line with a specific distortion function. Here, a skin distortion is applied in order to generate a real impression of the same synthetic finger. Figure 4.7 shows the pictorial representation of distorted fingerprint.

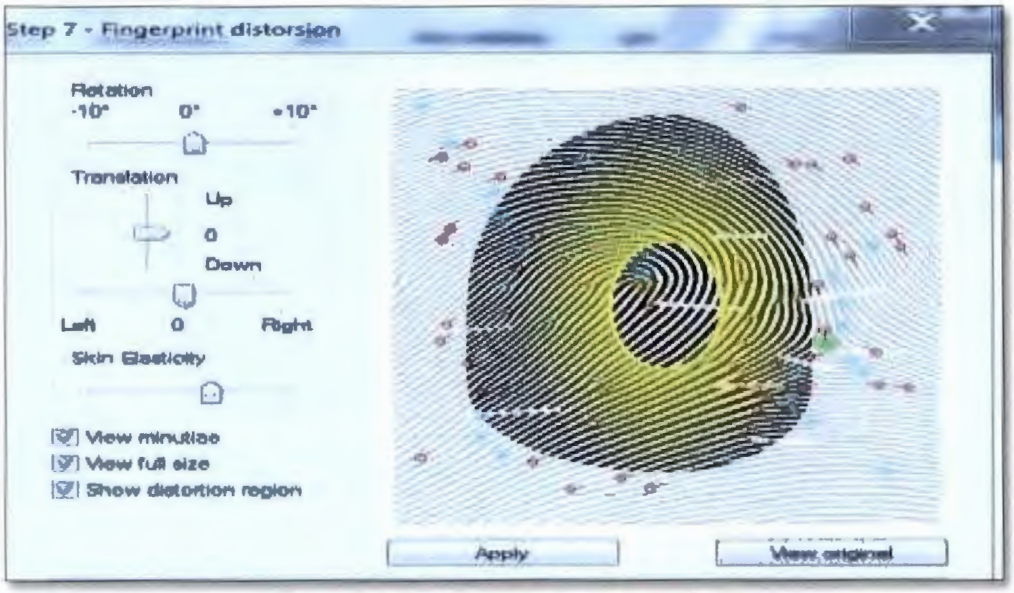

Figure 4.7: Fingerprint Distortion

4.2.6 Fingerprint Image Noising and Rendering

At this stage, noise and rendering texture is added to the master fingerprint in order to acquire certain impressions. The first stage is acquired without any form of noise and rendering texture and the second stage is acquired with both noise and rendering texture. The ridge pixels are subjected to certain from of deviation from the normal state in line with a specified noise and rendering level of which 3x3 average of filter is applied in order to smoothen the ridge pixels as shown in figure 4.8.

Figure 4.8: Fingerprint Noising and Rendering

4.2.7 Fingerprint Rotation and Translation

This interface showed in the Figure 4.9 describes the outcome of rotation and translation actions. A fingerprint image is generated by randomly rotating and translating the left loop classification of the master fingerprint. This is achieved by not cantering the fingerprint completely at the centre.

Figure 4.9: Fingerprint Rotation and Translation

4.2.8 Fingerprint Background and Contrast

This is the last stage in the generation of a fingerprint. The capacitive feature of the background is selected and applied on the master fingerprint in order to generate a background of the real form of the fingerprint, Figure 4.10.

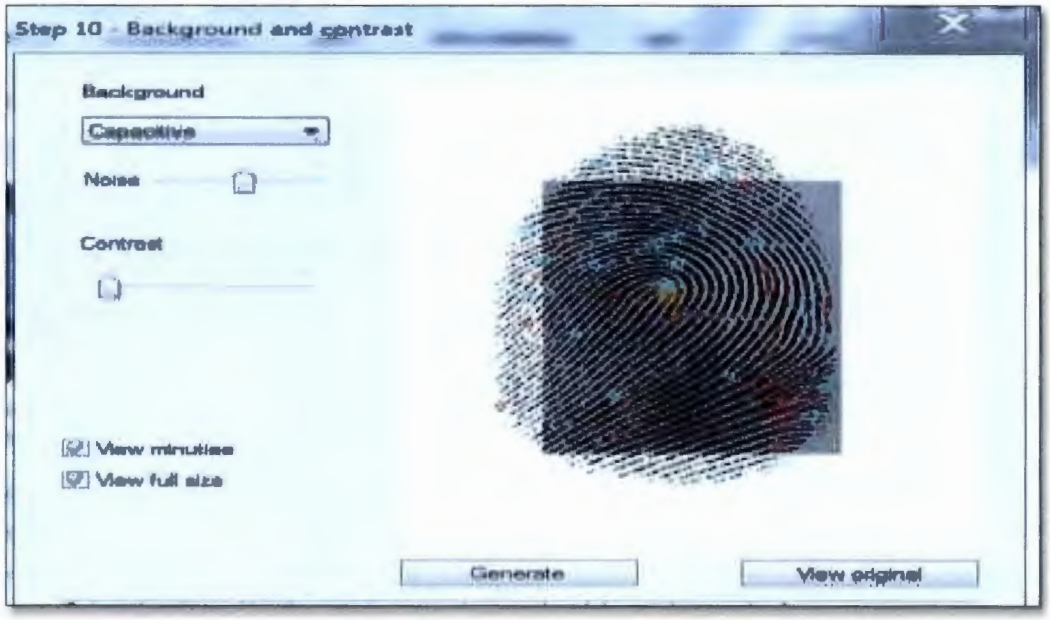

Figure 4.10: Fingerprint Background and Contrast

4.2.9 Fingerprint Left Loop

The Figure 4.11 indicates the left loop classification of the fingerprint. It is the final outcome of the synthetic fingerprint generation software tool. This is achieved by applying the transforming capability of the SfinGe to generate the actual background that is put at background.

Figure 4.11: Actual Fingerprint

4.3 MATLAB Fingerprint Image Processing

MATLAB is acronym for Matrix laboratory, see Figure 4.12. It has a computation, visualization and programing environment component and has the ability to integrate between them. It is a high performance language that can be used in technical computation. It can be used with ease because of its inbuilt data structures, editing tool and debugging.

```
Start// Algorithm for MATLAB Image Processing for generating Original/Actual fingerprint
//for minutia extraction
Input: Original/Actual Fingerprint Image
Expected Output: Extracted Minutia Point
Method: Template Matching
1. Perform Histogram Equalization
2. Perform Fast Fourier Equalization
3. Divide Image into Block Sizes
4. Extracting of Region of Interest
5. Display Result
6. Stop
```

Figure 4.12: MATLAB Actual Fingerprint Image Processing Algorithm

At this stage of extracting the region of interest (ROI), several operations such as Ridge Thinning, Minutiae Extraction, Removal of False minutiae and Minutiae Presentation will be performed in order to extract the actual minutiae point.

4.3.1 Gaussian Noise Fingerprint Image

In this image the Gaussian noise is added to the fingerprint image in order to express alterations and adjustments. The functions *imread* and *imnoise* are used respectively to add noise to the original image, see Figure 4.13.

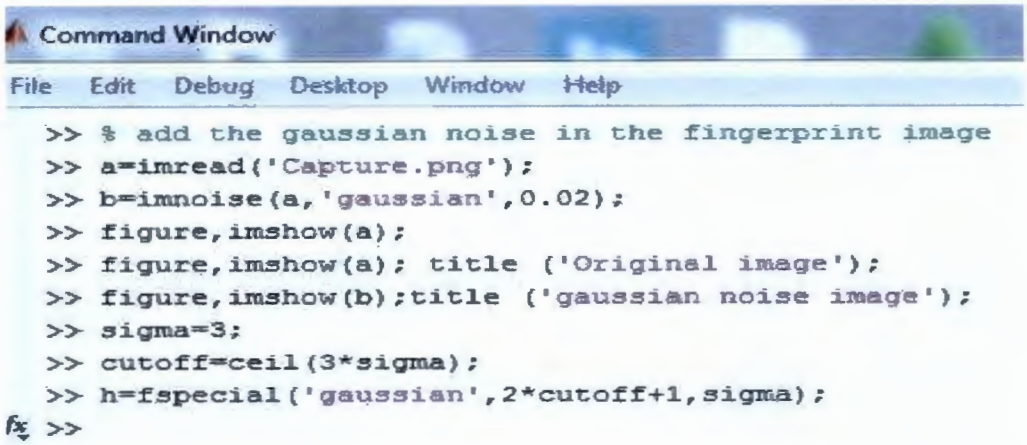

Figure 4.13: Gaussian Noise Image

4.3.2 Input of Fingerprint Image

The inbuilt MATLAB code is used to load the fingerprint image. The function *i=imread Capture.png* recalls the image from the stored folder, see Figure 4.14.

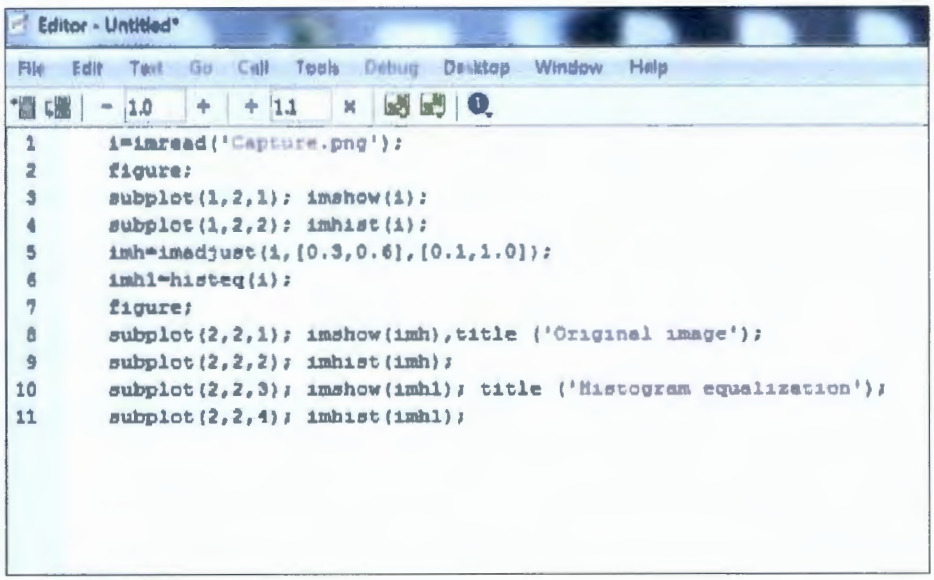

Figure 4.14: Loading Original Fingerprint Image

4.3.3 Fingerprint Image and Histogram Equalization

The histogram equalization is used to analyse an image, adjust its brightness, contrast and equalize the image. Histogram Equalization is performed in MATLAB using the function

imhisteq. The original histogram of the actual fingerprint image together with the equalised histogram of the fingerprint is reported in Figure 4.15.

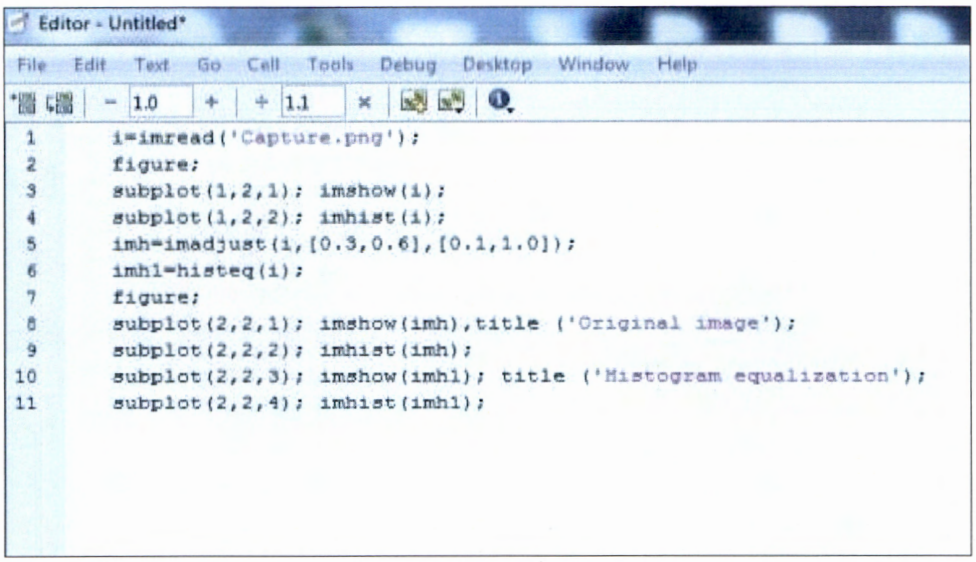

Figure 4.15: Original Fingerprint and its Histogram Equalization

4.3.4 Fingerprint Image Binarization

The *binarization* process of the fingerprint image is expressed in the Figure 4.16. It is achieved in MATLAB using the function *im2bw*. It involves the mapping of grey scale level image to a black and white image or binary image. In the MATLAB, the values 0, and 1 is used to represent the black and white respectively. The process is also used to adjust the greys scale image into binary. The threshold process is applied to an image, each pixel value analysed to the input threshold. A locally adaptive *binarization* process is performed to *binarze* the fingerprint image. The image is separated into specific blocks such as (16x16), and the mean intensity value is calculated for each of the blocks, which turns each of pixels into pixel 1 when the value of the intensity is larger than the mean intensity value of the current block that the pixel is attached to, see Figure 4.16.

```
232      %-------------------------------------------------------------------------
233
234      %Binary Image
235      % --- Executes on button press in binarize.
236      function binarize_Callback(hObject, eventdata, handles)
237      % hObject    handle to binarize (see GCBO)
238      % eventdata  reserved - to be defined in a future version of MATLAB
239      % handles    structure with handles and user data (see GUIDATA)
240
241 -    OriginalImage = imread('sample1.bmp')
242
243 -    MeanFilter = fspecial ('average', [3 3])
244
245 -    FilteredImage = imfilter (OriginalImage,MeanFilter);
246
247 -    NoiseImage = imnoise (OriginalImage,'gaussian',0.01,0.0)
248
249 -    BinaryImage = im2bw (NoiseImage,0.5)
250
251 -    subplot (1,4,3), imshow(BinaryImage), title ('Binarized Image')
252      %subplot (1,4,2), imhist(e), title ('Noise Histogram')
253
254
```

Figure 4.16: Original/Actual fingerprint Image and the Binary Image

4.3.5 Fingerprint Ridge Thinning

The thinning process is expressed in the figure below. Thinning is applied to the *binarized* image alongside the main pre-processing techniques that reduces the thickness of all the ridge lines into a single pixel with each of them becoming one pixel thick. The function *bwmorph* is used to achieve this. This code in the Figure 3.17 below is for the fingerprint image thinning, it explain the thinning image process that is applied after *binarization* and another major pre-processing technique which reduces the thickness of all ridge lines to a single pixel. Fingerprint identification or recognition thinning is done to thin the ridges so that each is one pixel thick. The algorithm removes the thickness with (3*3) little image widow whenever the fingerprint image is scanned, until eventually all the marked pixels are completely removed after series scan. The *thin* morphological operation in MATLAB is used to filter the thinned ridge as well as remove, isolated points, spike, and breaks.

```
255     %-------------------------------------------------------------------------
256     %Thinning Image
257
258     % --- Executes on button press in thinImage.
259     function thinImage_Callback(hObject, eventdata, handles)
260     % hObject    handle to thinImage (see GCBO)
261     % eventdata  reserved - to be defined in a future version of MATLAB
262     % handles    structure with handles and user data (see GUIDATA)
263
264 -   OriginalImage = imread('sample1.bmp')
265
266 -   MeanFilter = fspecial ('average', [3 3])
267
268 -   FilteredImage = imfilter (OriginalImage,MeanFilter);
269
270 -   NoiseImage = imnoise (OriginalImage,'gaussian',0.01,0.0)
271
272 -   BinaryImage = im2bw (NoiseImage,0.5)
273
274 -   ThinnedImage = bwmorph (BinaryImage,'remove')
275
276     %f = bwmorph (e,'thin', Inf)
277
278 -   imshow (ThinnedImage)
279
```

Figure 4.17: Thinning Image

4.3.6 Block Direction Estimation

The direction block of each of the pixel is assumed for the fingerprint image to be *M*M* pixel in size. It is estimated using the following algorithm as shown in Figure 4.18.

Start// Algorithm for obtaining the directional block of each of the pixel of the fingerprint image
1. Calculate the gradient value along x direction (gx) and y direction for ach pixel
2. Use "Sobel filters" to calculate the task
3. Use the tan2ß = 2 X ΣΣ (gx*gy)/ ΣΣ (gx2-gy2)
4. Display Result
5. Stop

Figure 4.18: Block Direction Estimation Algorithm

This formula implements the gradient value along x-direction and y-direction using Sine and Cosine value. The tangent value of the block direction can be then generated via Sine and Cosine values - $\tan 2\beta = 2\sin\beta \cos\beta / (\cos 2\beta - \sin 2\beta)$. When each of the block direction are executed, the blocks that do not have valuable information about the furrows and the ridges are eliminated using the formula - $E = \{2 \Sigma \Sigma (gx*gy) + \Sigma \Sigma (gx2-gy2)\} / M*M*\Sigma\Sigma (gx2+gy2)$, see Figure 4.18 and 4.19.

```
Command Window
>> % Block Direction Estimation
I=imread('Capture.png');
i=rgb2gray(I);
u=imresize(i, [256 256]);
t=graythresh(u);
u=im2bw(u,t);
figure
imshow(u);
[w,h]=size(u);
direct=zeros(w,h);
g_times_v=zeros(w,h);
g_sq_minus_v=zeros(w,h);
g_for_bg_under=zeros(w,h);
w=16;
sum_value=1;
bg_certanity=0;
times_value=0;
minus_value=0;
>> % blockIndex=zeros(ceil(w/W),ceil(h/W));
>> center=[];
>> filter_g=fspecial('sobel');
>> % to get gx
>> I_hor=filter2(filter_g,u);
>> % to get gy
>> filter_g=transpose(filter_g);
>> I_vert=filter2(filter_g,u);
>> g_times_v =I_hor.*I_vert; %gx.*gy
>> g_sq_minus_v=((I_hor-I_vert).*(I_hor-I_vert));%(gx^2-gy^2)
g_for_bg_under=((I_hor.*I_hor)+(I_vert.*I_vert));%(gx^2+gy^2)
>> %wAOp1=floor(w/W)*W;
%h1=floor(h/W)*W;
 for i=1:W:w;
for j=1:W:h;
times_value=sum(sum(g_times_v(i:i+W-1,j:j+W-1)));
minus_value=sum(sum(g_sq_minus_v(i:i+W-1,j:j+W-1)));
sum_value=sum(sum(g_for_bg_under(i:i+W-1,j:j+W-1)));
bg_certainty=0;
thet= 0;
if sum_value ~= 0 & times_value ~=0
  %  bg_certainty = (((2*times_value) + minus_value./256*sum_value);
   %bg_certainty = (((2*times_value)  + minus_value)/256*sum_value);
     bg_certainty = (times_value*times_value + minus_value*minus_value)/(W*W*sum_value);
     if bg_certainty > 0.05

         blockIndex(ceil(i/W),ceil(j/W))=1;
tan_value = atan2(2*times_value,minus_value);
      thet= (tan_value)/2 ;
      thet= theta+pi/2;
      center = [center;[round(i + (W-1)/2),round(j + (W-1)/2),theta]];
Start
```

Figure 4.19: Block Direction Estimation

4.3.7 Fast Fourier Transformation

The code in the Figure 4.19 shows how the input fingerprint is loaded as well as executing the *2D fft* MATLAB function in order to illustrates code of the input fingerprint is loaded and do the *(2D fft)* MATLAB function to decide the magnitude to display the fingerprint. Using the code *fft* displays the fingerprint at the centre and shifts fft to the centre and displays it.

The image is double converted with double precision floating point and it is brought within the range of *0 and 1* by the MATLAB function *mat2gray* and also the function i*m2unit8* to convert the values back to *0, 255* and the to the general log transformation.

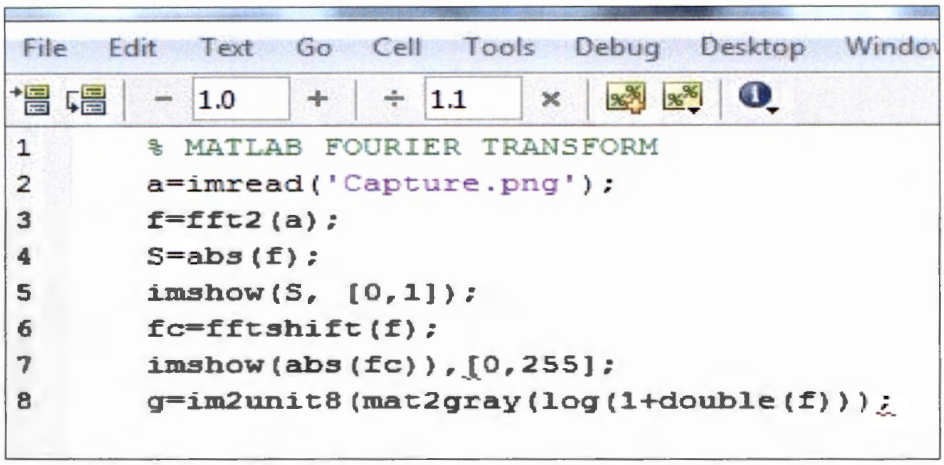

Figure 4.20: Fourier Transformation

4.3.8 Minutiae Image Extraction

The codes in the Figure 4.21 show how the minutiae image extraction is performed and stored for later use. After *binarization* and *thinning* of the image, the minutiae are extracted using the estimated region which includes ridge end finding and bifurcation. Ridge end is the location where a particular ridge terminates and bifurcation is the location at which one ridge splits into two ridges. These two features are very significant in determining minutiae points.

```
a=imread('Capture.png');
figure,imshow(a),title ('Input Image');
% convert to Input Image to binary image
b_i=im2bw(bw);
Undefined function or variable 'bw'.

b_=im2bw(a);
%% thinning image
t_i=bwmorph(b_i, 'thin',inf);
figure,imshow(t_i),title ('Thinned Image');
%minutiae extraction
s=size(t_i);
N=3; % window size
n=(N-1)/2;
r=s(1)+2*n;
c=s(2)+2*n;
double temp(r,c);
temp=zeros(r,c); bifurcation=zeros(r,c); ridge=zeros(r,c);
temp((n+1):(end-n),n+1:(end-n))=t_i(:,:);
outImg=zeros(r,c,3); % for Display
outImg(:,:,1)=temp.*255;
outImg(:,:,2)=temp.*255;
outImg(:,:,3)=temp.*255;
for x=(n+1+10): (s(1)+n-10)
        for y=(n+1+10): (s(2)+n-10)
            e=1;
      for k=x-n:x+n
         f=1;
            for b=y-n:y+n
 mat(e,f)=temp(k,b);
f=f+b;
            end
e=e+b;
      end;
      if(mat(2,2)==0)
          ridge(x,y)=sum(sum(~mat));
          bifurcation(x,y)=sum(sum(~mat));
      end
        end;
end;
%Ridge end finding
[ridge_x ridge_y]=find(ridge==2);
len=length(ridge_x);
% for display
for i=1:len
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),2:3)=0;
    outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;
    outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),2:3)=0;

     outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)-3),1)=255;
     outImg((ridge_x(i)-3):(ridge_x(i)+3),(ridge_y(i)+3),1)=255;
     outImg((ridge_x(i)-3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
     outImg((ridge_x(i)+3),(ridge_y(i)-3):(ridge_y(i)+3),1)=255;
end
%Bifurcation finding
[bifurcation_x bifurcation_y]=find(bifurcation==4);
len=length(bifurcation_x);
%For Display
for i=1:len
outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)-3),1:2)=0;
outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),1:2)=0;
outImg((bifurcation_x(i)-3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),1:2)=0;
outImg((bifurcation_x(i)+3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),1:2)=0;

outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)-3),3)=255;
outImg((bifurcation_x(i)-3):(bifurcation_x(i)+3),(bifurcation_y(i)+3),3)=255;
outImg((bifurcation_x(i)-3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),3)=255;
 outImg((bifurcation_x(i)+3),(bifurcation_y(i)-3):(bifurcation_y(i)+3),3)=255;
end
figure;imshow(outImg);title('Minutiae');
```

Figure 4.21: Minutiae Image Extraction

4.3.9 Region of interest (ROI)

Here, the region of interest (ROI), is used select or specify the subset or area of the fingerprint sample that is of interest. That is the identified area that can be used in matching. The code in the Figure 4.22 is used to indicate how it was done.

```
Command Window
>> %Read Input Image
>> InputImage=imread('Capture.png');
>> % Resize the Image
>> InputImage=imresize(InputImage,[256 256]);
>> % Display the Image
>> imshow(InputImage);
>> % Get Inputs from mouse, select 4 seed points in Image
>> [Col Row]=ginput(4);

c=Col;
r=Row;
% select polygonal region of interest
BinaryMask=roipoly(InputImage,c,r);
figure, imshow(BinaryMask); title('selected Region Of Interest');
>> %Create Buffer for ROI
>> ROI=zeros(256,256);
>> %Create Buffer for NONROI
>> NONROI=zeros(256,256);
for i=1:256

for j=1:256

if BinaryMask(i,j)==1
ROI(i,j)=InputImage(i,j);

else
NONROI(i,j)=InputImage(i,j);
end

end

end
>> %Display ROI and Non ROI
>> figure;
subplot(1,2,1);imshow(ROI,[]); title('ROI');
>> subplot(1,2,2);imshow(NONROI,[]); title('NON ROI');
```

Figure 4.22: ROI

4.4 Results Analysis

The implementation was carried out with MATLAB source code. Therefore, the analysis was reported with two kinds of filtering such as; mean and median filtering in addition of White Gaussian noise.

4.4.1 Loading Actual Fingerprint Image

The Figure 4.23 shows the full image of the original/actual fingerprint generated from to SfinGe Software which was implemented with the MATLAB code using the function *Capture.png*.

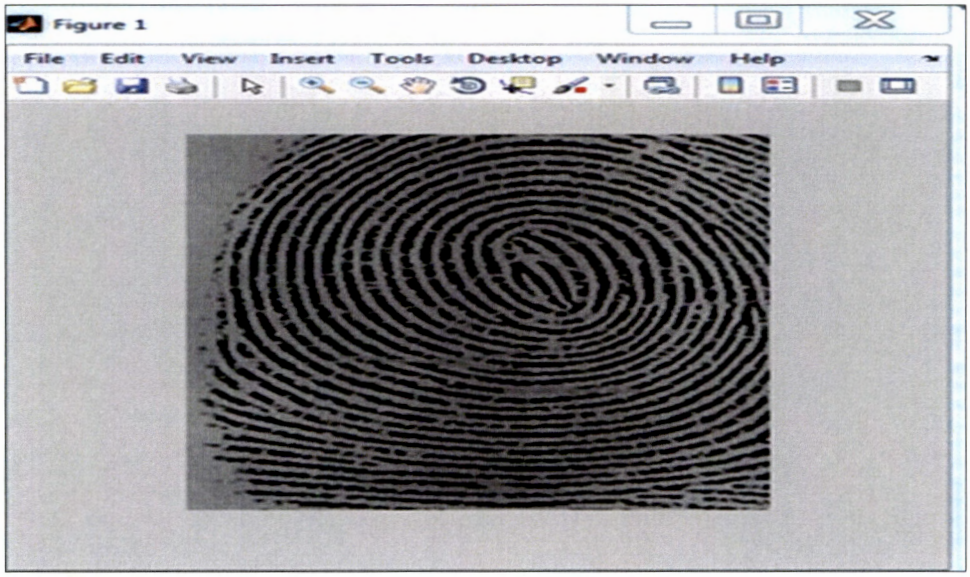

Figure 4.23: Original/Actual Fingerprint Image

4.4.2 Fingerprint Histogram Equalization

The Figure 4.24 is the result obtained when the MATLAB code for histogram equalization was executed. The pixel distribution of the fingerprint imaged was increased and the enhancement and virtual effect also increased.

Figure 4.24: Fingerprint Histogram Equalization

4.4.3 Fingerprint Image with Noise

Figure 4.25 shows the fingerprint image that is interrupted by noise. The Gaussian noise was accomplished by using MATLAB function: *imnoise (0.02).* The noise was loaded at an average mean of 0.02 and a default variance of 0.00. Where Gaussian Noise is the output image and Original/Actual fingerprint image is the input image, with parameters 0 as the default mean value and 0.01 as the variance value. Evidently, we can see that from the original image histogram have less white pixels, as the number of the white pixels is over 200. On the other hand, when Gaussian white noise is added, we have a total of 255 white pixels as a result of white Gaussian noise.

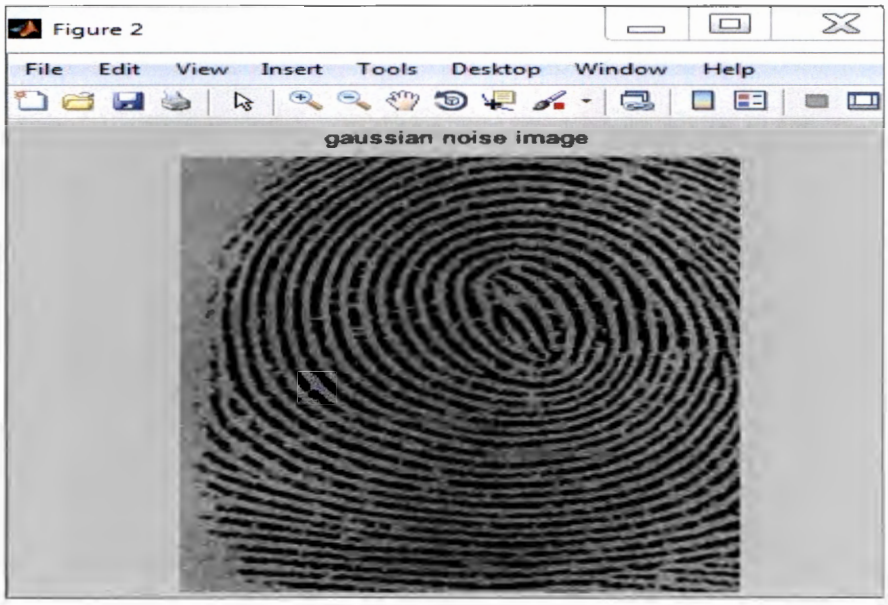

Figure 4.25: Gaussian Noise Image

4.4.4 Actual Fingerprint Histogram

The Figure 4.26 represents the results of the loading the actual fingerprint histogram. From the results on the graph it indicates that some pixels were lost due to the contrast modifications of the image of the histogram.

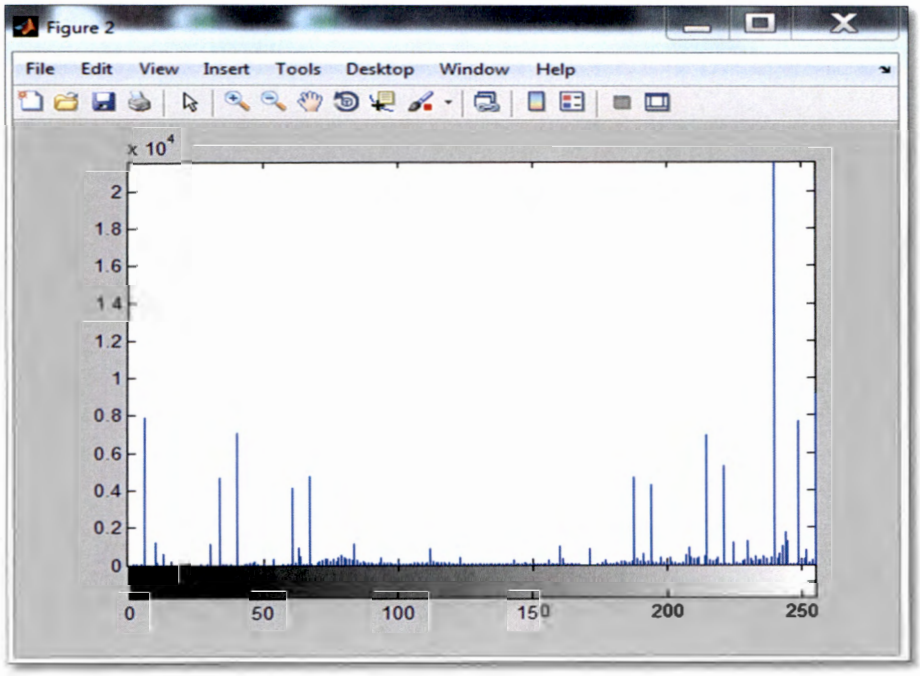

Figure 4.26: Actual /Original Fingerprint Histogram

4.4.5 Fingerprint Histogram Equalization

The figure 4.27 indicates the results obtained after executing the histogram equalization code in MATLAB. The adaptive threshold was determined and added on the image histogram. The region having a uniform intensity indicated an increase up to the strong peak in the histogram pixel above the histogram threshold.

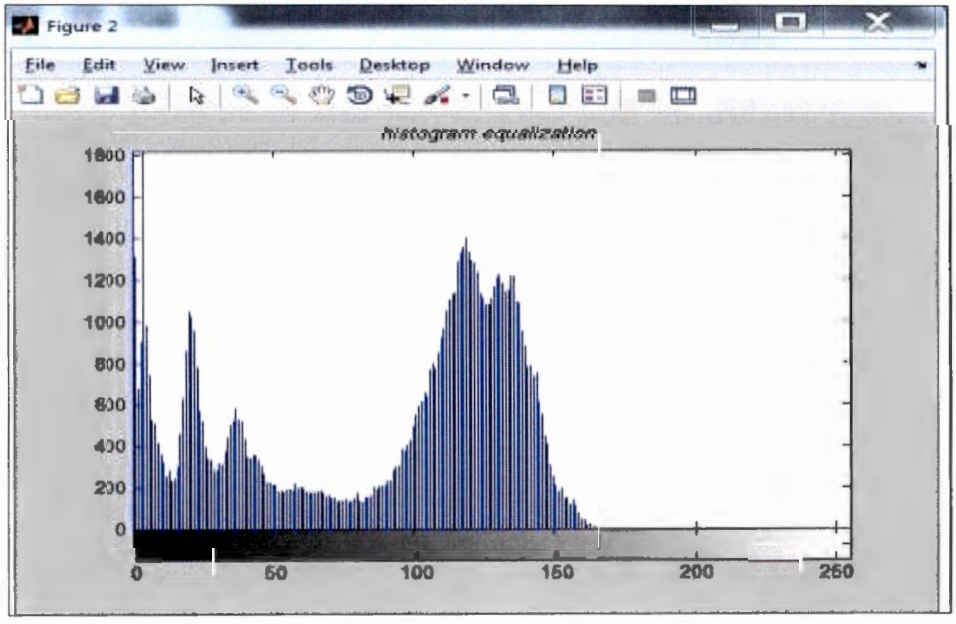

Figure 4.27: Histogram Equalization

4.4.6 Binary Image

The image below shows the results obtained from the image *binarization* code in figure 4.16, when executed in MATLAB. In performing the post filtering process, we have to *binarize* the image to convert the image to black and white and also remove the background to get the desired image. In order to achieve this we used the function *im2bw*. This adjustment of grey scale image to binary image was realised by performing the threshold process on the fingerprint image. When the threshold process is applied to the image, each pixel value is translated to the input threshold. The result is displayed in the Figure 4.28.

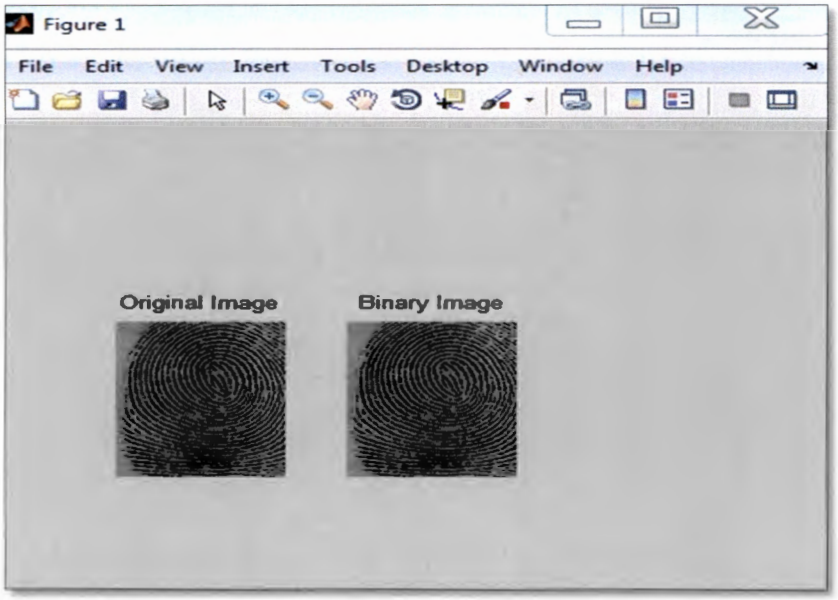

Figure 4.28: Original Image and Binary Image

4.4.7 Thinning Image

The Figure 4.29 shows the result obtained after running the code for fingerprint ridge thinning in MATLAB. When the enhancement process was performed on the image it was converted to binary and was loading for the thinning process which was achieved using the function *bwmorph*: *Thinning* = *bwmorph.* The interior pixels are removed; breaks are reduced, including isolated points and spurious ones, leaving behind an outline of the fingerprint image. We used this operation to extract a simple representation of regions and to obtain the shape of the fingerprint which can be used for extracting regions of interest such as the minutiae feature extraction.

Figure 4.29: Thinning Image

4.4.8 Fourier Transformation Image

The Figure 4.30 shows the results obtained from the code of Fourier transform image which was executed in MATLAB. From the outcome the image is separated into segment so as to enhance a specific block by dominant frequencies. 108

Figure 4.30: Fourier Transformation Image

4.4.9 Region of Interest Fingerprint Image

The Figure 4.31 shows the results obtained from the code for the fingerprint region of interest executed in MATLAB. The area of interest was indicated using a polygon-like structure. A

filtering operation was added to the region of interest image and a binary mask was created by setting the size of one of the pixels to 256 with the rest set to 0. The image process of NON ROI was set the same as ROI. The results obtained identified that the value of the intensities and the pixels are non-contiguous. The essence of this is to create a mask of the region because of sensitivity of the region of interest in the actual fingerprint identification process. It is used to perform the minutiae extraction. The ROI image aids in the identification and authentication of the system user.

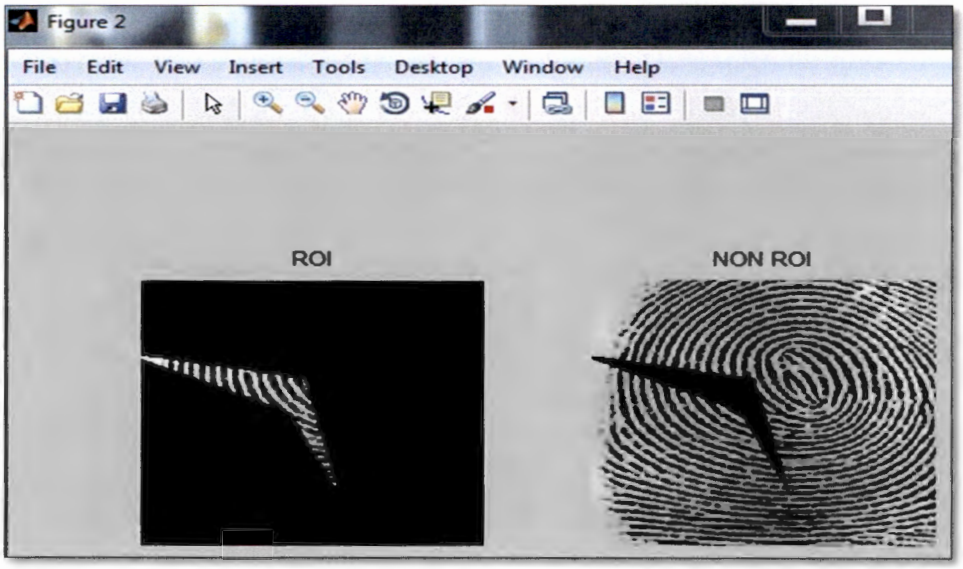

Figure 4.31: ROI and NON ROI

4.4.10 Minutiae Extraction Image

The Figure 4.32 shows the outcome of the execution of the code for minutiae extraction in MATLAB. After *binarization* and *thining* process the minutiae was extracted from the thinned ridge. The red spots indicate the ridge ending point while the green spots indicate the bifurcation of the ridge line. Minutiae are decided based on both ends of the ridges. Categorically, these features are called minutiae. Generally, we obtained this by first acquiring the image using the SFinGe software, and then create Gaussian white noise. When the filtering process is applied the ROI is obtained from which the minutiae are extracted. At this stage we assumed the image was ready for template matching.

Figure 4.32: Minutiae Extraction Image

4.5 Chapter Summary

In this chapter, we described in details the stages, algorithms and the tools employed to achieve the response to research question 2 and its corresponding objective. It involved generating and extracting the fingerprint minutiae point using the algorithms of fingerprint image processing. By these processes the unique features of a fingerprint are specified which enhance the security of the users profile in a biometrics authentication and identification system. These several stages were represented in source codes and were implemented in MATLAB software. The (SFinGe) software generated a sample of the fingerprint which formed the actual fingerprint which was run in the MATLAB for minutia point extraction.

Chapter 5

Fingerprint Minutiae Point Matching

5.1 Chapter Overview

This section presents the analysis of fingerprint biometrics minutiae point matching which is basically the stage where identification is determined after the analysis of minutiae extraction point has been successfully analysed.

5.2 Stages of Fingerprint Minutiae Matching

In order to determine that two fingerprints are from the same finger, the general pattern configuration must be compared and must align with each other. This means that the two fingerprints must have the same pattern configuration. The components of the Figure 5.1 presents below represent various stages involved in the fingerprint minutiae point matching.

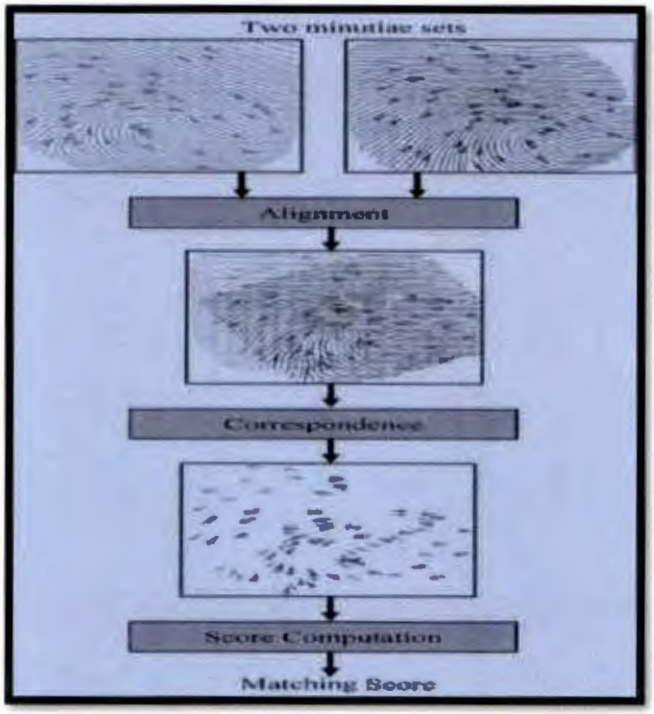

Figure 5.1: Fingerprint Minutiae Matching Stages

Categorically, the fingerprint matching process is executed using a three iterative process [132]. Firstly, two fingerprints that are matched and compared to determine if they are similar to each other, or whether they are completely different in terms of global pattern configuration, or if it is possible that the two fingerprints are from the same finger.

Secondly, a pattern alignment process is conducted in which feature points are initially located from the fingerprint before performing an appropriate alignment of the fingerprint. Thirdly, a matching process is conducted in which corresponding minutiae details are determined and evaluated within the valid fingerprint pattern areas and a decision is made based on corresponding pairs and pattern configuration identified.

However, as a result of the variations in the challenges we concluded that the quality of fingerprint impression deformation, fingerprint ridge configuration, and skin quality/condition, including several steps in fingerprint matching protocols cannot be clearly and precisely identified. Therefore, fingerprint examiners heavily depend on their experience to make decisions for conclusions. For instance, even in the most prominent minute details, minutiae cannot be identified and determined easily. Sometimes ridge bifurcations can even be identified as ridge endings when the impressions of the fingerprint are too low.

Conclusively, although fingerprint matching is conducted on a daily basis all over the world by numerous fingerprints matching systems, it still remains an art instead of a science. This is because in fingerprint matching, experience plays in the decision threshold.

The fingerprint templates are stored in the database to enable the matching module during the verification/ authentication, and identification stage. In the identification stage, the captured sample of the fingerprint is compared with the feature set of the templates created and stored in the database during enrolment for similarity. This is done in terms of the matching score and the system reference threshold. Where the matching score is lower than the already defined threshold in the database, the input fingerprint image is concluded to have matched successfully with the subject template then the person has been identified. This defined value determines if the individual is or is an imposter in any verification/ authentication, or identification system [144]. The threshold plays a very important part in deciding the authenticity of a user, by matching two fingerprint minutiae images for a biometric authentication and identification. Two fingerprint minutiae images are matched with a minutiae matching tool, after which a matching value/score is generated and later compared to the reference threshold score/value.

In real time biometric authentication system a database of biometric images is prepared. Furthermore, the threshold values of each individual fingerprint are also identified, and are used later in authentication and identification systems. The authentication process identifies

the authenticity of an individual using the decision threshold (FAR, FRR) values stored in the database.

5.2.1 Matching Model

Accuracy is an important aspect of an authentication system. It depends highly on the chosen values of the decision threshold. The fingerprint image (minutiae) extracted are stored in the database in vector form which are referred to as image points. The minutiae are automatically extracted and saved in the database through enrolment for verification, authentication and identification phases. The matching of a fingerprint using a matching model explains the level of similarity between two minutiae image points. In this thesis we applied the Euclidean Distance Model to determine the matching similarity. However, for the Euclidean Distance we used the computation of square root of the sum of the squares of the differences between two image vectors referred by (1).

$$ED = \sqrt{\sum_{k-1}^{m} (FV_{i,k} - FV_{i,k})^2} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where $FV_{i,k,}$ and$FV_{j,k}$, are minutiae image points having length [m, i, j] as the iterators on the minutia image points database. Applying Image Matching value of [0] shows that both minutiae image points belong to one individual and having a value approaching towards [0] shows that the two minutiae points are obtained from one individual. The Matching process is performed between two minutiae point images and the matching value/score also generated as a result obtained from the comparison. It is also determined based on the decision threshold value. The minutiae image points extracted are stored as image vectors. The figure below indicates that the matching score obtained should be less than or equal to the decision threshold, then the user can be determined as genuine. Thus it is represented as follows:

$$\left.\begin{array}{l} Matching\ Score\ \leq D_{TH} \\ Matching\ Score\ > D_{TH} \end{array}\right\} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Therefore, it becomes a fact that choosing the right value as the decision threshold is very significant in an authentication and identification system. Biometrics identification using the minutiae matching model (MMM) is an iterative process. Certain variations in various conditions between enrolment and identification phases in a biometrics system such as noise either temporary or permanent will never guarantee 100% match, as complete secured

systems are still far-fetched. Nevertheless, an enduring effort has been made to ensure that only the genuine users are granted access per time. Hence the rate of FRR is reduced to its barest minimum.

Consequently, in knowledge and token based authentication and identification systems, only 100% match is considered and any deviations can result into access being denied whereas, in a biometrics authentication and identification system, no determination line exist between a matching and a non-matching fingerprint. The determination for the matching is based on two data sets that are being matched. The probability percentage of matching is decided by the kind of biometrics system. Based on this, 100% accuracy cannot be realised on a biometrics systems. For this reason, forensic analysis is needed in some cases in order identify an impostor. As indicated in the Figures (Figure 5.2 and Figure 5.3) below, the genuineness of an individual depends largely on the matching score (MS) in any real time authentication system

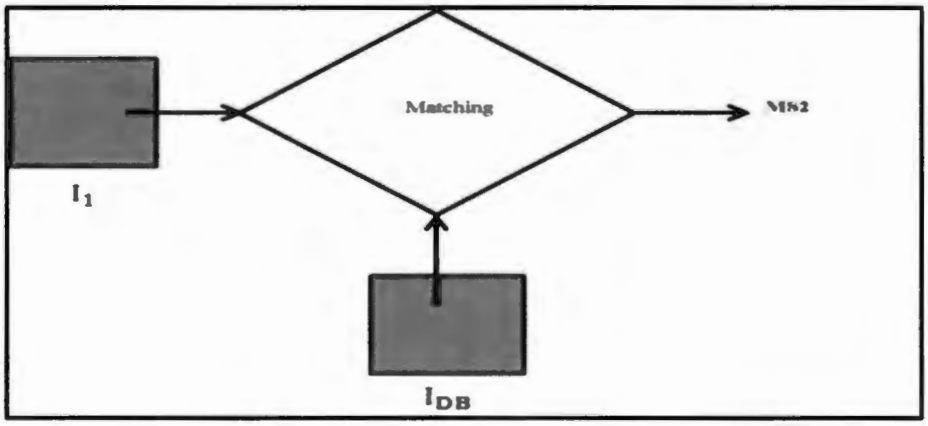

Figure 5.2: Matching of I_1 with I_DB 114

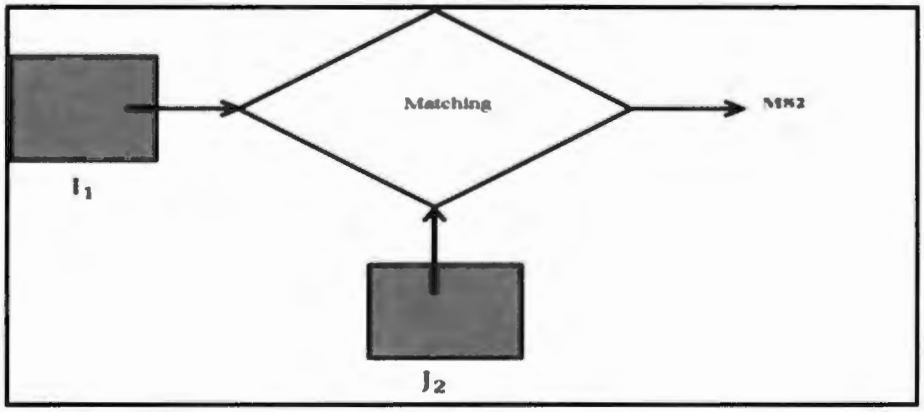

Figure 5.3: Matching of I_1with J_2

Basically, if the two fingerprints that are being matched are quite different, there will be some values on the matching score, and then the decision of the correct value for the decision threshold will basically differentiate the same fingerprints from another fingerprint and the conclusion can be reached. This shows the essence of choosing the right threshold value. Apart from the issues of possible attacks from impostors, when improper values for the decision threshold are selected, two possible errors can occur; false matches leading to false acceptance, and false non-matches leading to false rejection. It is a false match or false acceptance when an obtained template matches correctly to a template that is previously stored in the database, even though they are from two different individuals. It is a false non-match or false rejection when the obtained template does not correctly match with the template that is previously stored in the database, even though they are from the same individual. Moreover, error rates differ among various biometrics traits and also depend on the setting of the threshold value.

However, we assumed that the fingerprint database is segmented into two sets called S1 and S2.

Hence, B denotes the total number of each of the individuals' images stored in the database and N denoted the total number of individuals stored in the database. (M-1) fingerprint images form a category SI (System enrolment) for each individual as shown in (1) and one fingerprint image will form category S2 (Authentication/Identification) for each individual as shown in (2).

P1 Category:

$$F_I=\lfloor I_1, I_2 \ldots\ldots I_{(M-1)} \rfloor, F_2=\lfloor I_1, I_2 \ldots\ldots I_{(M-1)} \rfloor, \ldots\ldots F_N=\lfloor I_1, I_1, \ldots\ldots I_{(M-1)} \rfloor \cdots\cdots\cdots (3)$$

S2 Category:

$$F_I=\lfloor I_M \rfloor, F_2=\lfloor I_M \rfloor, \ldots . F_N = \lfloor I_M \rfloor \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (4)$$

where,

Fi represents ith individuals' in category S1, S2,
Ij represents the jth fingerprint image in category P1, P2,
M represents the number of fingerprint images of one individual stored in the database

The matching of F_1 images is performed using the diagrams below:

Hence, the matching among individuals fingerprint M_1 in phase $P1$ is shown in the Table 5.1.

Table 5.1: Minutiae Matching

i; j	*1*	*2*		*M-1*
1	*X*	MMM_{12}	...	$MMM_{1(M-1)}$
2	PMM_{21}	*X*	...	$MMM_{2(M-1)}$
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮
M-1	$MMM_{(M-1)2}$	$MMM_{(M-1)2}$		*X*

Similarly in Category S1 every minutiae fingerprint image vector represented in F_1 is

$$TA_1 \begin{bmatrix} MMM_{12} \\ MMM_{13} \\ \vdots \\ MMM_{IM-1} \\ MMM_{21} \\ \vdots \\ \vdots \\ MMM_{2M-1} \\ \vdots \\ \vdots \\ MMM_{(M-1)1} \\ MMM_{(M-1)2} \vdots \\ FMM_{(M-1)(1-2)} \end{bmatrix} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (5)$$

Similarly, every N fingerprint image samples matching outputs are stored in the database using the space called the decision threshold array DT_A reported in (6) and presented in the equation below:

$$T_A = TA_1 + TA_2 + TA_N \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (6)$$

Min and max matching values are identified by the array of decision threshold, such as

$TA1 + TA2 + \cdots\cdots TA_N$, For every person is reported in (7) shown below:

$$\begin{pmatrix} T_{AMIN} = min\langle T_A \rangle \\ T_{AMIN} = min\langle T_A \rangle \end{pmatrix} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (7)$$

Max and min threshold values from $TA\ are\ seperated\ into,\ NTH$ which is the rate of threshold values shown below, where MX=Maximum and MN= Minimum

$$\Delta = (T_{AMX} - T_{AMN}) / N_{DTH} \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (8)$$

$$\Delta 1 = T_{AMIN} + \Delta \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (9)$$

$$\Delta 2 = T_{AMIN} + 2\Delta \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (10)$$

Similarly, $\Delta N_{DTH} = T_{AMIN} + N_{DTH}\Delta \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (11)$

Consequently, in analysing all NTH values, we choose a decision threshold value for the system under some conditions: When FAR, and FRR are equal, when FAR is at minimum and at fixed values of FAR.

Going further, we assumed a fingerprint-based biometrics authentication and identification system in order to analytically explain the reference threshold calculation for any particular system. Therefore, we assumed the NWU Mafikeng Campus fingerprint database system. The database was grouped into S1 and S2, A total of 50 clients and having 6 print images for every individual. The S1 Category contained 5 clients' fingerprint images captured during enrolment stage and stored in the database while the S2 Category contained one client's fingerprint image that is utilised during the system's testing period. The size of the fingerprint image is assumed to be 284×384 pixels. The fingerprint image used is also assumed to be 64×64 pixels.

$$F_I = [I_1, I_2 I_3 I_4 I_5], F_2 = [I_1, I_2 I_3 I_4 I_5], F_{50} = [I_1, I_2 I_3 I_4 I_5] \ldots\ldots\ldots\ldots\ldots (12)$$

Apparently, in S1 Category each fingerprint Fi consists of five (5) sample images *I-5* given at (14)

S2 Category:

$$F_I = [I_6], F_2 = [I_6], \ldots\ldots\ldots F_{50} = [I_6] \ldots\ldots\ldots\ldots\ldots (13)$$

Also in the S2 Category each of the fingerprints contains only sample image 6 given at (16). The fingerprints minutiae points were extracted using the minutiae extraction algorithm and the matching of the minutiae images were performed using Euclidean distance. In S1 category, each fingerprint image vector in F_I was matched with the rest of the four (4)

fingerprint image vectors using Euclidian distance minutiae method and the matching scores were stored in distance threshold array. Similarly, for all the 50 fingerprints image samples, 1000, matching values were stored in threshold array (TA) given by (6)

$$T_A = TA_1 + TA_2 + \cdots\cdots\cdots\cdots\cdots\cdots TA_{50}$$

The minimum and maximum matching values were seen in the decision threshold arrays (TA1, TA2 ...TAN) for 50 individuals and were stored in the database.

$$\left.\begin{matrix} T_{AMIN} = \min(T_{Ai}) \\ T_{AMAX} = max\ T_{Ai} \end{matrix}\right\} (i = 1, \ldots 100)$$

The maximum and minimum matching values were seen in the decision threshold arrays (TA) for determining the decision threshold value given by (7).

$$T_{AMIN} = \min(T_A),\ T_{AMAX} = \max(T_A)$$

The minimum and maximum values of the decision threshold arrays were divided into 11 threshold values using (8-11).

$$\Delta = (T_{AMAX} - T_{AMIN})/\ 11$$

$$\Delta 1 = T_{AMIN} + \Delta$$

$$\Delta 2 = T_{AMIN} + 2\Delta$$

Similarly, $\Delta 11 = T_{AMIN} + 11\Delta$

5.3. Measuring Metrics (FRR and FAR) at different thresholds

In this study the measurement of False Rejection Rate (FAR) and False Acceptance Rate (FRR) metrics were used to conduct the matching/comparison. Table 5.2 below indicates the various metrics used and their respective threshold values. The table contains 11 threshold values which were tested with Category C2 and Category C1 images. The value of the decision threshold was chosen were where FAR is minimum. The operating point for fingerprint authentication and identification system was considered at the value of FAR, see Table 5.2..

Table 5.2: FRR and FAR Evaluation

No of the fingerprint	Threshold	FAR	FRR
1	0	2	60
2	0.5	5	40
3	1	7	20
4	1.5	14	10
5	1.1	5	225
6	1.15	3	30
7	1.2	2	35
8	1.25	1	40
9	1.3	1.5	45
10	1.35	0	100

The Figure 5.4 below shows the result of the FAR/FRR at their respective thresholds. The value of FRR on the threshold indicated that decrease in threshold results in an increase in the number of FRR. This is because of the rate of low threshold matches which are "true" which means that there is a high rate of FRR. However, the decrease in threshold occurred as a result of noise and other factors that affected the system which are not identified by the system.

On the other hand the false acceptance rate of impostors resulted in a lot of errors than false rejection rate. Therefore, we conclude that it is preferable for a system to keep FAR to its barest minimum. This can be achieved by setting a low threshold closer to the one where only the matches are identified and the rest are rejected. This means that the higher the system's security level, the lower the threshold needed to maintain it.

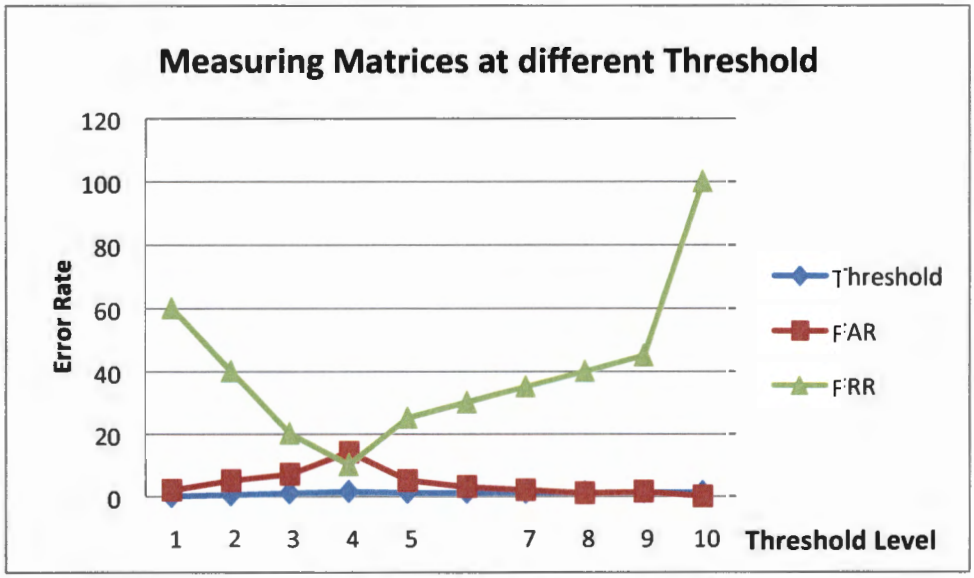

Figure 5.4: FRR and FAR graph

5.3.1 Decision Threshold

For a fingerprint to be accepted or rejected depends largely on the matching score falling above or below the threshold. This threshold can be adjusted so that in a biometrics authentication system the rate of FAR and FRR can be less or more depending on the requirements of the biometric system.

The table below shows the results obtained when determining FAR and FRR. The threshold was kept to a maximum of 1.35 to avoid the increase in FRR. From the figure we observe that there are very low values of FAR for all values of FRR. The aim is to as much as possible have a low FAR for small values of FRR.

Table 5.3: Values of FAR and FRR

Threshold	FAR	FRR
1.25	2	36
1.3	6	26
1.35	7	10
1.4	5	6
1.9	8	1.3

When FRR is above 20% is concluded to be really high; therefore in order to reduce the false rejection rate, the threshold level should be increased.

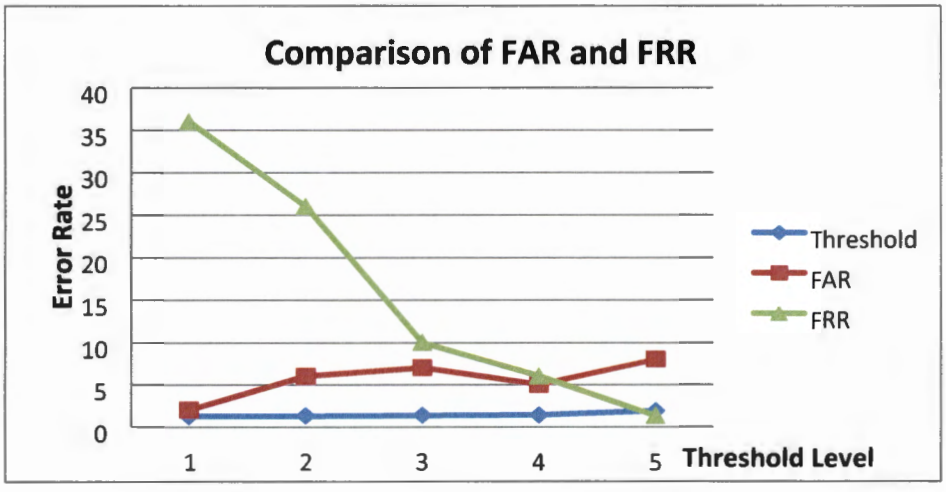

Figure 5.6: Comparison of False Rejection Rate (FAR) and False Acceptance Rate (FRR)

Figure 5.6 shows a graph of hard coded values of FAR and FRR. Small values of FAR make it possible for imposters to attack the system, while high values of FRR makes it possible to identify unauthorized people.

5.4 Chapter Summary

In this chapter, we described analytically in details the stages involved in performing fingerprint minutiae point matching. The various stages included Stages of Fingerprint Minutiae Matching, Matching Model Design, Measuring Metrics (FRR and FAR) at different thresholds, Decision Threshold, Comparison of False Rejection Rate (FRR) and False Acceptance Rate (FAR). Also discussed in this chapter are the challenges often times encountered during fingerprint minutiae point matching.

Chapter 6

Design and Implementation of Biometrics Authentication Technology

6.1 Chapter Overview

This chapter provides the practical aspects of biometric technology. It consists of the requirements, analysis, implementation and result analysis of the prototype biometric fingerprint authentication and identification system that enhances information security and network management. This is achieved by transforming the information from the system specifications component analysis reported in chapter 4. This system can effectively record the student's" attendance using their fingerprint. Moreover, NWU was used as the implementation domain. Also, reported in this chapter are the interface relationships that describe the operation and different functionalities of the biometrics system as specified in the requirements and use case diagrams presented in Table 6.2 below. This chapter also includes system capability and deployment criteria, system impacts and benefits as well as system vulnerabilities and threats.

6.2 Biometric Authentication/Identification System Flowchart

The Biometrics Authentication/Identification System Flowchart below consists of two main components which include the enrolment of the user biometrics by the use of a biometrics sensor into the database, and the authentication of the user using the captured biometric.

This interface provides a mechanism for a user to indicate his/her identity and present his/her fingerprint to the system. Depending on the type of application the interface can be designed to fit the practical requirements. In the prototype verification system, FTIR fingerprint scanners are used to acquire the live-scan fingerprint images as shown in Figure 6.3.

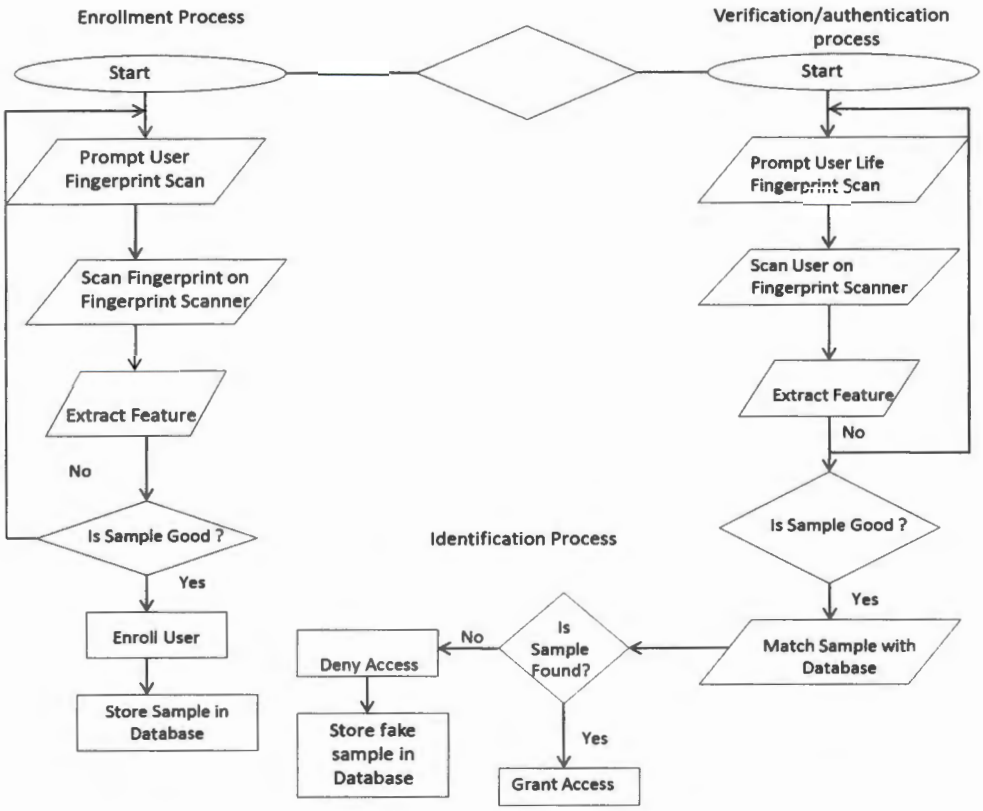

Figure 6.1: Biometric Identification System Flowchart

Consequently, the individual's/user's fingerprints and details/profile is enrolled into the system database. To enhance performance and efficiency, an expressive biometrics technology/method is used. The extraction s made from the raw digital representation of the fingerprint. When the profile of the user/ individual is presented to the system in the enrolment module, the feature extraction algorithm is applied to the fingerprint image, the minutiae patterns of the fingerprints are extracted and transmitted through the quality algorithm checker to ensure that a good quality should be stored in the system database. A default value of a good quality fingerprint is 25 for genuine minutiae to be detected. The major responsibility of the verification module is authentication. The individual (subject) places the finger on the scanner and a digital image of the fingerprint is captured and the minutiae pattern is extracted from the captured fingerprint image and transmits it to the minutiae matching algorithm which performs a matching against the minutiae template of the individual (subject) stored in the system database.

Similarly, the system database is a collection of records (fingerprint and students name) of the authorized genuine users of the systems. These individuals should be allowed access to the system.

Each user record has some information which is used for authentication purposes such as the user's profile which includes the name and student number, and fingerprint template. The system database can be either a physical database that is embedded in the system or virtual database that has the details of the users inscribed in the magnetic card issued to the/every individual (user). A typical example is an ATM card, a system where the authentication is conducted by the point of access, the client/user presents his/her identity by entering the user name and the system retrieves the corresponding details contained in the database for verification and authentication. In this case it is not practically feasible to have a database which stores all the records because a large template database may increase failure (technical failure). Therefore for information security applications such as the ATM voting cards it is generally more efficient to have the records/details stored on magnetic cards while the users are in custody of their cards.

However, at the point of access the user provides the magnetic card for the system for identification which further requests the biometrics feature for identification. The template database in this case is a virtual database. No physical database exists in the system because they are already stored in the magnetic cards. In this sole verification system, the number of template and their quality are paramount design parameters. Several templates can be stored for every user, and the more the templates, the more researches required and it obviously increases the efficiency and the performance of the system.

6.2.1 System Level Design

The systems level design depends on the biometrics characteristics or features to be used. It involves the enrolment and sensor module earlier explained. This constitutes the major challenges in the system level design, including the operational mode to be used, how a raw digital representation of a biometrics feature is to be acquired, the architecture of the system, and other issues like ergonomics, physical size, power supply, weight, cost, administrative and maintenance cost and the environmental influences. The biometrics feature to be selected or used especially the performance requirements, practical performance requirement is highly application related. The primary objective maybe the low false reject (LFR) which is seen from the system accuracy view point. In forensic applications like criminal identifications, the major concern is the false reject rate (FRR) and not the false acceptance rate (FAR). This means that in examination missing a criminal event at the expense of examining a large number of potential matches identified by the biometrics system is not our desire. The human

expert makes the final decision and conclusion in forensic applications. On the other hand in any secure access control application the main objective is to prevent impostors, even though the concern of biometrics is to determine possible inconveniences to the legitimate users due to the high false rate. There are several applications in which the false acceptance rate and the false rejection rate are to be considered. A typical example is the ATM card verification where the false rejection rate is more important than the false acceptance rate. Having a false acceptance rate means a lot of financial losses and a high false rejection rate will so much irritate the clients. In civilian application, a high false acceptance rate is not preferred or desired because the primary aim / advantage /benefits of automation is defeated if human experts still have to manually examine a large number of false positives generally from automatic verification and identification systems.

Typically, it is ideal to have a reliable binary output that ensures the subject is in the system database. However, a high rate of false rejection is also not generally desirable because that would give impostors access to the system. But in forensic (criminal or security) applications, the risk involved is much more severe [82, 88].

Categorically, some biometrics features or characteristics are very good at accepting genuine individuals but in preventing impostors they do not perform well. For instance an individual may easily be mistaken as a result of changes in make-up, hair style, lighting conditions, background and so on. Also, there are biometrics features/ characteristics like/such as the retina scans, fingerprint and Iris scan that are better at determining impostors but they are not efficient in determining genuine users or clients. Also, the hand geometry and the hand vein which perform in a similar manner in preventing impostors and admitting/ accepting genuine users [84, 90]. Generally, there is no -basic rule that determines which biometrics technique should be used for a particular application. An appropriate and realistic design strategy is to critically examine the system requirements, and selected the techniques that are suitable for a particular application and align the biometrics system to satisfy the practical performance requirements. Practically, a biometrics system can operate either as a verification system or an identification system. In a verification system the system accuracy is the main challenge. Because it is only open to one comparison is conducted, it is not usually, so difficult to meet the response time requirement of a verification system whereas in identification system both accuracy and speed is initially required.

Therefore, in comparison, designing an identification system is much more difficult than a verification system. An identification system explores the entire template database in order to establish an identity. Thus, the feature extraction holds more required information especially the feature matching aspect. Inherently, some biometrics techniques operate better in the identification mode than others. For instance, the local minutiae details and their relationships of a fingerprint mainly determine the individuality of fingerprints. To match an unregistered fingerprint is computationally realizable though expensive. Fingerprint classification can proffer a practical slight solution to indexing a fingerprint database because just a linear research of a whole template database is not acceptable [134].

Therefore, using dedicated hardware devices for matching and efficient indexing mechanisms, a real time search on a relatively small sized fingerprint database containing thousands of fingerprint images can be conducted effectively. It is also feasible to design a face recognition system that operates in the identification mood. The reason is because face comparison is a less expensive operation and secondly, efficient/effective indexing techniques are available and the recognition performance is admissible in court. Though an identification system is very expensive and requires more resources, it is more accepted and adopted than the verification system [53]. Generally, an operational standard for any biometrics systems depends largely on the practical requirements and identification system is usually not technically practical. The ATM card identification system is a typical example. It is required to connect all the ATM machines around the world, establish a template to establish a template database with millions of records and also must be able to search through millions of templates records in real time for even access authentication. For this reason, data acquisition is one of the critical processes on a biometric system. This selection of a data acquisition device depends mainly on the practical requirements of the system which include availability, cost and size. No specific rules exist that determine the type of device to use. Any efficient/ reliable device can be used to acquire the biometrics images from every individual. Thus, in this thesis, our concentration was on fingerprint biometrics feature. The type of application determines the type of biometrics system architecture to be implemented. Categorically/Logically, every biometrics system must consist of the enrolment module and the identification module. Relatively, each of the two modules consists of other sequential sub modules. Each sub modules consists of input from the previous sub modules and produces intermediate outputs which are in turn used as inputs for the next sub modules. Basically, the design of the sub modules in the system is determined by the type of biometrics

feature being used. Thus, in this thesis, our concentration was on the fingerprint biometrics feature, which we used to design a fingerprint biometrics attendance system. However, the system level design is much tightly related to the algorithm level design, and it represents the enrolment sensor module

6.2.2 Algorithm Level Design

Having specified the system level and the practical requirements, the next major challenge is the algorithm design. This level design involves the minutiae extraction module, matching/comparison module, and decision module. The feature extraction stage abstracts the representative features belonging to the same source. The algorithm level design also includes other modules such as database management, quality control, encryption, as well as user interphase. Fingerprint representation features makes up the essence of algorithm level design. Almost every aspect of fingerprint recognition mechanism systems are determined by the fingerprint representation features. A presentation consists of two main properties such as saliency and suitability. By saliency is meant that every representation must contain enough class specific (information) about the input data while suitability means that the representation can easily be extracted and stored in a compact manner and kept useful for matching. Generally a matching algorithm is based on a similarity basis/function in order to determine if two sets of features are from the same finger. Deriving a similarity function from the same fingerprint for a particular representation is difficult due to the intra class and interclass variations. Categorically, no symmetric way exists by which we can derive a similarity function. In automatic fingerprint identification, the acquired image usually has redundancy and large intra class variations. Two main representative mechanisms exist for automatic fingerprint identification. They are referred to as image-based representations and feature-based representations. Image-based representations ascertain that the individuality of fingerprints is determined exhaustively within the spatial or frequency domain. For instance a fingerprint can be represented by its Fourier spectrum. Because fingerprint has orientation specific flow pattern of ridges its concise representation may be obtained using the Fourier spectrum. The image-based representation usually requires that input enrolled image be registered by its Fourier spectrum. This registration has been proposed in literature yet the validity of this representation is still far from being corroborated [135].

The feature-based representation specifies that a pair of fingerprints belongs to the same category such as the arc, loop, short and other features and shares a large number of

significant level ridge features, then confidently we can conclude that they are from the same finger. Feature-based representation of fingerprints has been widely accepted by the automatic fingerprint identification community because the validity has proven beyond reasonable doubt by all results obtained from the practical operations of automatic fingerprint identification systems that use it [85][136].

6.2.3 Authentication/ identification Level Design

This level design involves- database and decision making module earlier explained. In this thesis, we focused on verification system which uses only fingerprints in identity authentication. It conducts only one on one comparison to authenticate whether the identity claimed by an individual is true or not. This system is designed mainly for applications such as ATM card security, smart card security, information system security and access control applications. Consequently, this thesis presents our prototype attendance system. This system essentially consists of four main components such as: user interface, enrolment module, system database, and authentication module.

It is basically developed for implementing fingerprint authentication and identification to enable attack or any form of anomaly discovery. On the other hand if any anomaly is discovered, digital forensic analysis process can then be employed in order to identify who the impostor is. The four main components such as: user interface, system database, enrolment module and an authentication module [137].

i. User Interface Module: This interface provides a mechanism for a user to indicate his/her identity and present his/her fingerprint to the system. Depending on the type of application the interface can be designed to fit the practical requirements. Figure 4.2 shows our prototype authentication system flowchart.

ii. The enrolment module: Here the individuals/user's fingerprints and details/profile are/is enrolled into the system database. To enhance performance and efficiency, an expressive biometrics technology/method is used. The extraction is made from the raw digital representation of the fingerprint. When the profile of the user/ individual is presented to the system in the enrolment module, the feature extraction algorithm is applied to the fingerprint image, the minutiae patterns of the fingerprint are extracted and transmitted through the quality algorithm checker to ensure that a good quality should be stored in the system database (default value of

a good quality fingerprint is 25 for genuine minutiae to be detected). The major responsibility of the verification module is authentication. The individual (subject) places the finger on the scanner and a digital image of the fingerprint is captured and the minutia pattern is extracted from the captured fingerprint image is stored in the database. Moreover, the analysis of our minutiae point extraction was reported in chapter 5 of this thesis. It is also transmitted to the minutiae matching algorithm which performs a matching against the minutiae template of the individual (subject) stored in the system database to check if the claimed identity is correct or not.

iii. System Database Module: The system database is a collection of records (fingerprint and student's name) of the authorized genuine users of the system. These individuals should be allowed access to the system. Each user record has information which is used for authentication purposes such as the user's profile which includes the name, student number, and fingerprint template. The system database can either be a physical database that is embedded in the system or a virtual database that has the details of the users inscribed on the magnetic card issued to the/every individual (user). A typical example is an ATM card, a system where the authentication is conducted by the point of access, the client/user presents his/her identity by entering the user name and the system retrieves the corresponding details contained in the database for verification and authentication. In this case it is not practically feasible to have a database which stores all the records because a large template database may increase failure (technical failure). Therefore for information security applications such as the ATM voting cards it is generally more efficient to have the records/details stored on magnetic cards while the users are in custody of their cards. However, at the point of access the user provides the magnetic card for the system for identification which further requests for the biometric feature for identification. The template database in this case is a virtual database. No physical database exists in the system because they are already stored in the magnetic cards. In this sole verification system, the number of template and their quality are paramount design parameters. Several templates can be stored for every user, and the more the templates, the more researches required and it obviously increases the efficiency and the performance of the system. But our prototype biometric attendance system designed, and analysed in chapter 5 of

this thesis has a database which means that there is a physical database that is embedded in the system.

6.3 Biometric System Deployment

The decision on where to deploy the biometrics authentication system within the university or any company or organization is very important for effective and efficient impact. Planners or the administration must select a deployment strategy that is based on careful analysis of the institution. The network policy and information security requirements that support the operational functionality and maintenance of the system should be developed. However based on our findings from this study some deployment domains are recommended including the ones already stated in the course of our discussion.

- Location 1: At the main entrance to the premises
- Location 2: At the lecture venues
- Location 3: At the entrance to the laboratories or restricted areas
- Location 4: At places designated for general usage.

Basically, the principles discussed in the sections above are the exact fundamentals of a biometrics authentication system in a real time environment. Therefore, we have reported the prototype system in the next phase/stage. We did not implement all the components as it were because of the constraints involved in the prototype systems.

6.4 Analysis and Design Phase

In this section, we presented the Rational of the system, System Requirements Definition, Use Case Descriptions, Activity Diagrams, and Database Design respectively.

6.4.1 Rational of the System

This segment of this thesis presents an authentication scenario where the university students are to use fingerprint scanners to prove that they are attending lectures and they are not illegal students. This will motivate the students to be disciplined and punctual. The attendance is usually taken using attendance registers provided by the lecturers in class and not the system. Using this traditional system the students cheat by asking their friends to write their names or tick for them because they want to meet the requirement of 80% attendance that qualifies them to seat for the semester examination. The lecturers are not able to monitor the students to ensure that they are writing their names only. Therefore it is difficult for the lecturers to

keep accurate records of the students' attendance. This makes the traditional means less efficient. This thesis intends to design a system that can effectively record the students' attendance using their fingerprint. This will be introduced at lectures and laboratories. The system will take the attendance at both the beginning and at the end of the lectures to ensure that the students attend the lecture and were in class till the end of the lecture period. However, the fingerprint used in this system is assumed to have gone through the fingerprint minutiae point extraction processes to acquire the region of interest that is stored in the database.

On the other hand, if each and every student, staff, and visitors has their fingerprint collected and stored in the database, it would be easy and possible to forensically analyse all incidents of security breaches or misconduct that occurred on or within the campus if necessary and have the right impostor or offenders identified and properly prosecuted.

6.4.2 System Requirements Definition

From the above specification we identify system actors then draw up a use case diagram which is then accompanied by use case descriptions of each identified use cases.

Table 6.1: System Requirement Definition

Id	Requirements	Priority
	FUNCTIONAL	
1	The system shall accept biometrics for authentication.	
2	It shall grant access to specific areas based on fingerprints.	
3	The system shall allow the system administrator to create and view user accounts.	
4	The system shall allow the school administrator to create venue time tables.	
5	The system shall allow the school administrator to register students.	
6	The school administrator will be able to create modules.	
7	The system shall create attendance registers for each attended module.	
8	Each lecture shall be granted a privilege to view their attendance registers.	
9	Each user shall be authenticated before being granted access to the system.	
	NON FUNCTIONAL	
10	The system shall be easily accessible from the web	
11	The system shall use a language that is more secure	
12	The system response time shall be very minimal	
13	The system shall consume a few resources as possible (space and time)	

The actors of the system are students, Lecturers, System Administrators and the School administrators.

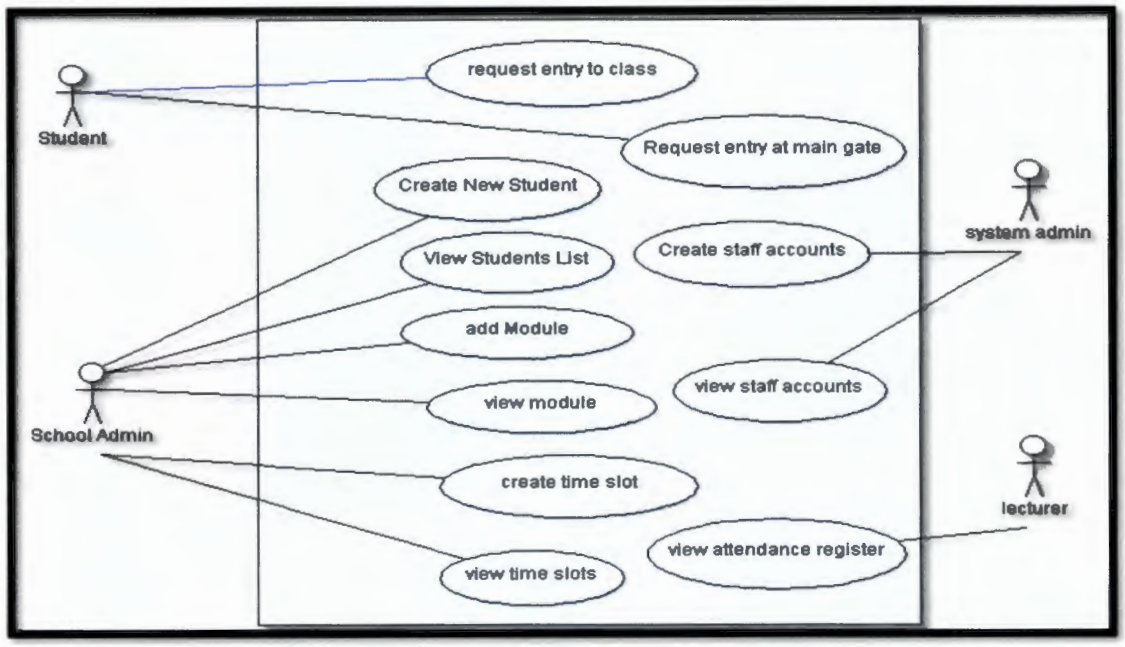

Figure 6.2: Use Case Diagram for the Biometric System

6.4.3 Use Case Descriptions

This section of the requirements analysis provides a vivid description of the biometrics system using use case. It shows how information in the system and network is processed and controlled.

6.4.3.1 For Entry Request

This represents the use case description table for entry request. It consists of 2 columns and 17 rows. The column contains the use case ID (USE CASE ID) and the row contains use case number (Uc1). The objects of the columns and the rows are also indicated respectively.

Table 6.2: Use Case Description for Entry Request

USE CASE ID	Uc1		
Use Case Name	Entry Request (Finger Print Authentication)		
Created By	Ohaeri I.U.	Last Updated By	Ohaeri I.U
Date Created	10/05/2015	Last Revision date	19/05/2015
Actors	Student		
Description	Every time the student enters a demarcated area or attends class they are asked to scan their finger prints for authentication purposes.		
Trigger	Student requests entry		
Preconditions			
Post Conditions	1. Student has been granted access		
Normal flow	1. Student requests access 2. The student provides biometric details 3. The system authenticates the student 4. Access is granted		
Alternative flow	4a the student is not registered 1. Access is denied 4b The venue is not supposed to be in use 1. Access denied		
Exceptions			
Includes			
Frequency of use	High		
Special requirements			
Assumptions	1. Students submitted biometric details during registration 2. Electricity is not a problem to the academic institution.		
Notes and issues			

6.4.3.2 For Register Student

This represents the use case description table to register students. It consists of 2 columns and 12 rows. The column contains the use case ID (USE CASE ID) and the row contains the use case number (Uc2). The objects of the table are indicated here:

Table 6.3: Register Student

USE CASE ID	**Uc2**		
Use Case Name	**Entry Request (Finger Print Authentication)**		
Created By	Ohaeri I.U	**Last Updated By**	Ohaeri I.U.
Date Created	10/05/2015	**Last Revision date**	19/05/2015
Actors	School Administrator		
Description	Every enrolled student has to have their details captured into the system		
Trigger	Student request Registration		
Preconditions	Application has been accepted		
Post Conditions	2. Student is registered		
Normal flow	1. Student requests registration 2. The administrator enter personal details 3. The student is asked to submit biometric details 4. The system registers module of selected degree 5. Student details are persisted		
Frequency of use	High		
Assumptions	3. Students has been accepted		

6.4.3.3 For the Create Module

This represents the use case description table for the create module. It consists of 2 columns and 12 rows. The column contains the use case ID (USE CASE ID) and the row contains use case number (Uc3). The objects of the columns and the rows are also indicated respectively.

Table 6.4: Create Module

USE CASE ID	Uc4		
Use Case Name	**Create Time slot**		
Created By	Ohaeri I.U	**Last Updated By**	Ohaeri.I.U.
Date Created	10/05/2015	**Last Revision date**	19/05/2015
Actors	School administrator		
Description	A time slot is some sort of a venue time table that specifies which module is to be attended at what time		
Trigger	Request for new time slot		
Preconditions	1. The venue exists 2. Modules have been created		
Post Conditions	2. Time slot included in time table		
Normal flow	4. User opens the new time slot form 5. User adds specific details 6. The details are stored into the database		
Frequency of use	Low		
Assumptions			

6.4.3.4 For Create Time Slot

This represents the use case description table for create time slot. It consists of 2 columns and 13 rows. The column contains the use case ID (USE CASE ID) and the row contains the use case number (Uc4). The objects of the columns and the rows are also indicated respectively.

Table 6.5: Create Time Slot

USE CASE ID	Uc5		
Use Case Name	**Create Account**		
Created By	Ohaeri .I.U	**Last Updated By**	Ohaeri.I.U
Date Created	10/05/2015	**Last Revision date**	19/05/2015
Actors	System administrator		
Description	Each system user has to have a unique account in order to be able to access the system		
Trigger	Request for account		
Preconditions	1. The user is an employee in the institution		
Post Conditions	1. The user has an account		
Normal flow	1. The actor opens the new account form 2. He/she adds specific user details 3. The details are stored into the database		
Frequency of use	Medium		
Assumptions			

6.4.3.5 For Create Account

This represents the use case description table for entry request. It consists of 2 columns and 12 rows. The column contains the use case ID (USE CASE ID) and the row contains use case number (Uc5). The objects of the columns and the rows are also indicated respectively.

Table 6.6: Create Account

USE CASE ID	Uc5		
Use Case Name	**Create Account**		
Created By	Ohaeri .I.U	**Last Updated By**	Ohaeri.I.U
Date Created	10/05/2015	**Last Revision date**	19/05/2015
Actors	System administrator		
Description	Each system user has to have a unique account in order to be able to access the system		
Trigger	Request for account		
Preconditions	1. The user is an employee in the institution		
Post Conditions	1. The user has an account		
Normal flow	1. The actor opens the new account form 2. He/she adds specific user details 3. The details are stored into the database		
Frequency of use	Medium		
Assumptions			

6.4.3.6 For View Attendance

This represents the use case description table for view attendance. It consists of 2 columns and 12 rows. The column contains the use case ID (USE CASE ID) and the row use case number (Uc6). The objects of the columns and the rows are also indicated respectively.

Table 6.7: View Attendance

USE CASE ID	Uc6		
Use Case Name	**View attendance**		
Created By	Ohaeri I.U	**Last Updated By**	Ohaeri.I.U
Date Created	10/05/2015	**Last Revision date**	19/05/2015
Actors	Lecturer		
Description	On entry into a venue each student is recorded and this information is used to generate an attendance report which lecturers have access to.		
Trigger	Lecture request for an attendance register		
Preconditions	Lecture is logged into the system		
Post Conditions	1. A specific Attendance register is displayed		
Normal flow	1. The lecture selects the module of choice		
	2. The lecture then selects a specific date 3. The system generate a report		
Frequency of use	High		
Assumptions	There were students who attended the module at that particular date.		

6.4.4 Activity Diagrams

Activity diagrams are diagrams that capture the dynamic characteristics of a system; in this section we transform the most important use cases of this system which involve biometrics authentication into activity diagrams, see Figure 6.2.

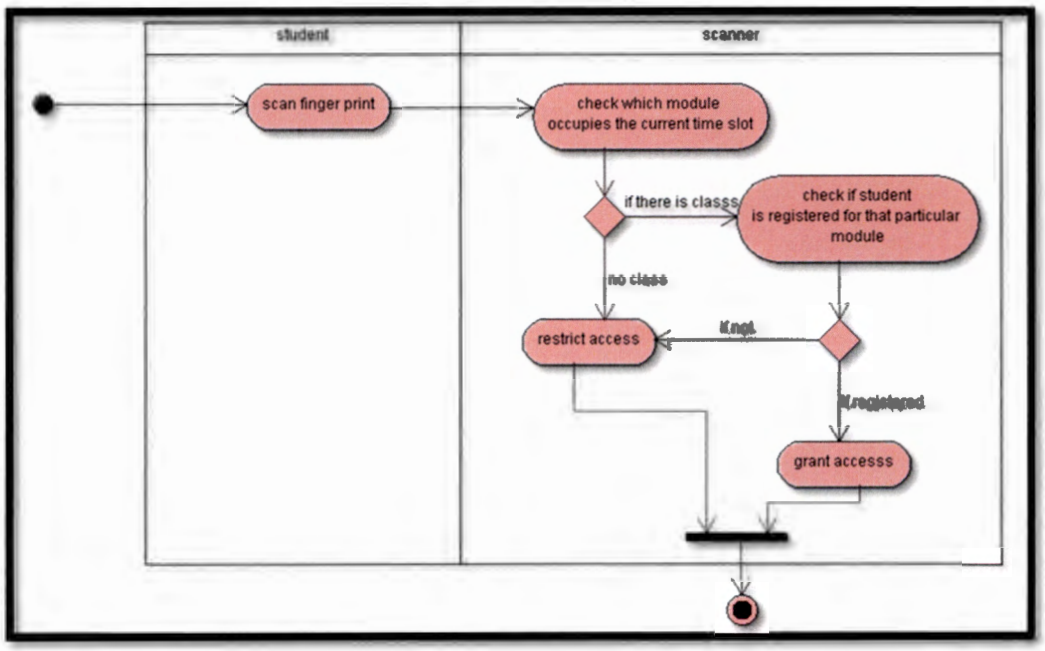

Figure 6.3: Activity Diagram for Authentication Process at a Lecture Venue

For a student to be granted access to a specific venue, that student has to be registered for the module that occupies the time slot at hand. This effectively means that the system has to maintain a timetable for each venue. When a student requests access the system compares the current time and the time frames in the time table then get the module that is to be attended, The system then confirms if the student is registered for that particular module, if they are registered then access is granted if not access is denied. If the current time slot is vacant no one is allowed in. This is represented in Figure 6.2 above.

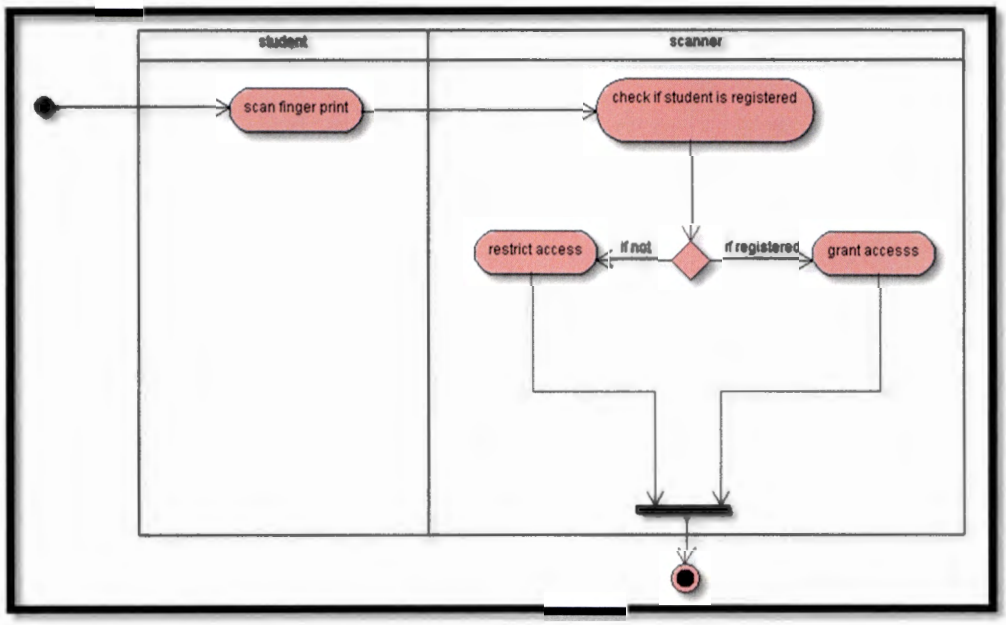

Figure 6.4: Activity Diagram for Authentication Process at the Gate

The Figure 6.3 shows the flow of events as a student authenticates at the gate. On registration each student submits biometrics details, thus at the gate they scan their fingerprint which is then searched for from the database, if it is found the person is granted access if not, access is denied.

6.5. Database Design

The data base schema was created using SQL and the RDBMS of choice was MySQL. Below is a list of the business rules that were used to create the schema.

i. The university provide more than one degree

ii. Each degree has more than one module

iii. Each student has to be registered

iv. Each student registration contains one or more modules

v. All staff member have to have one and only one account

vi. The university has a record of class venues

vii. Each venue is allocated one or more modules

viii. Each venue has a time table

ix. Only one module can be attended per time interval

The diagram below shows the resulting database schema

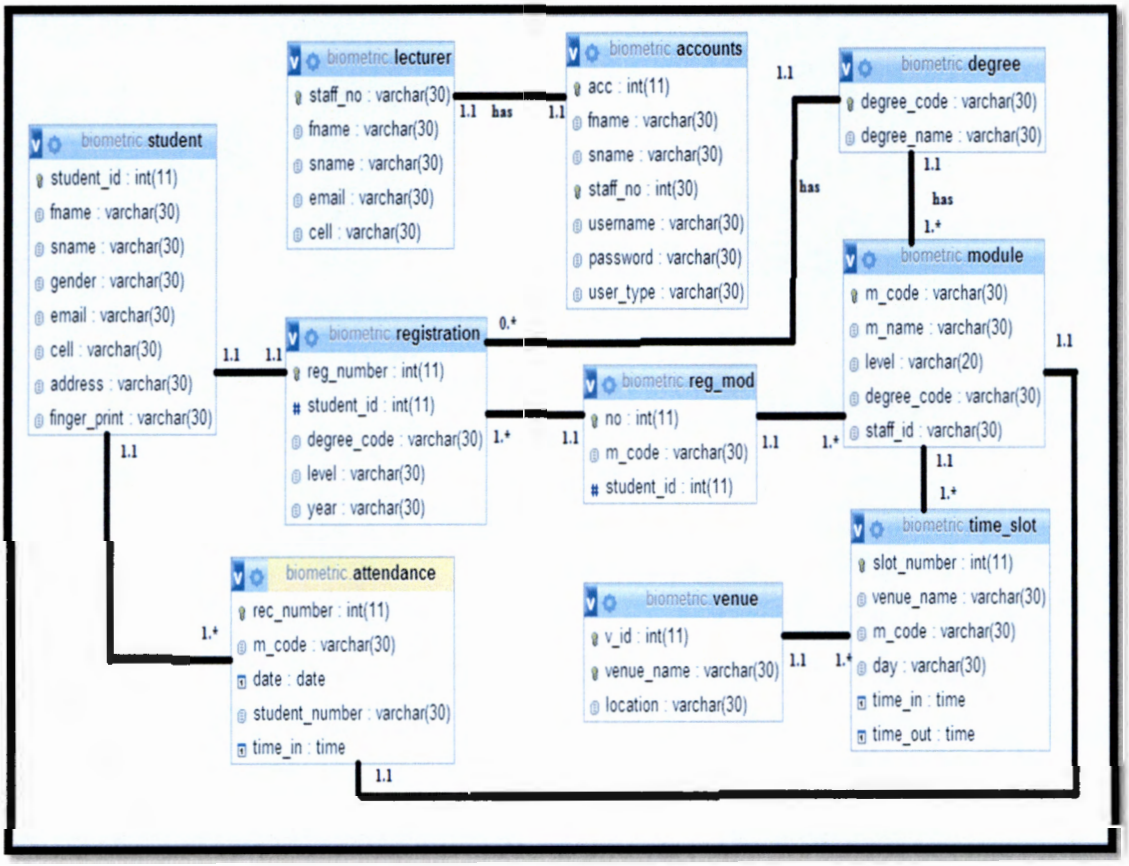

Figure 6.5: Biometric System Database Schema

6.6 System Implementation Phase

In this section, we presented System Interfaces, System Administrator Interface, School Administrator Interface, and Lecturer Interface.

6.6.1 System Interfaces

This section describes the interface of the biometrics system. This system was created using two languages Java and PHP. Java was used to develop the scanning software prototypes then the rest of the system was developed in PHP and run on the web.

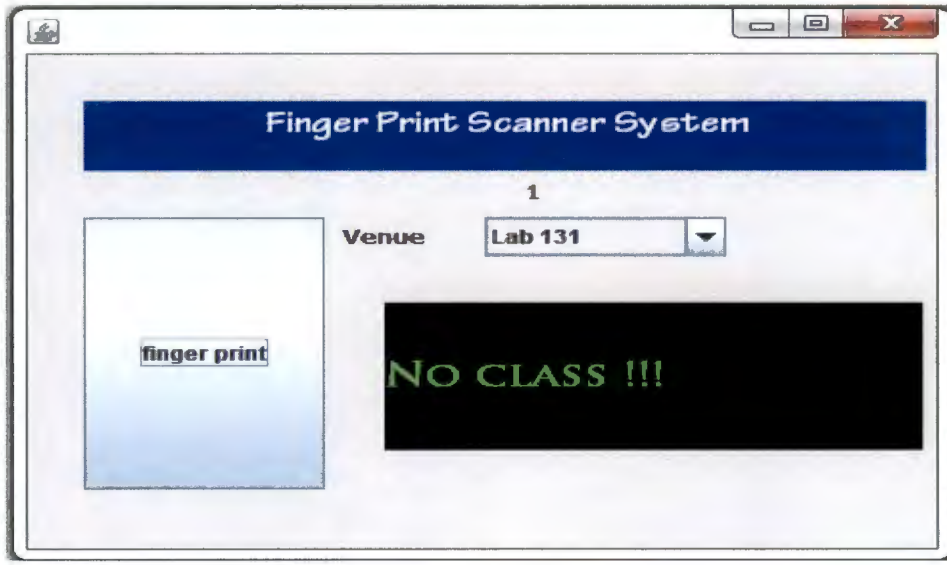

Figure 6.6: Venue Scanner

The interface shown in Figure 6.5 represents the scanner to be installed at each lecture venue. The interface has a scanning portion which appears on the left then a large display that gives feed back to the user.

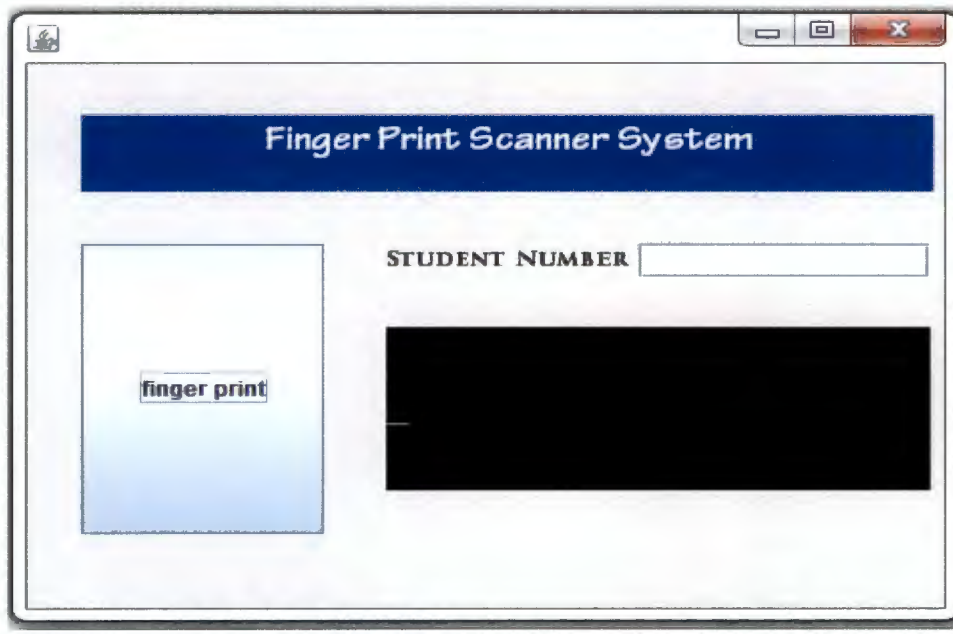

Figure 6.7: Scanner Located at the Entrance

The interface shown in Figure 6.6 represents the scanner at the gate. The scanner will have the above interface, the fingerprint input space is to the left then there is a student number label that will display the student number after scanning and just below that is the feedback display.

The above interfaces were coded in java then the ones that follow below were coded in html and C++, thus then run on web browsers.

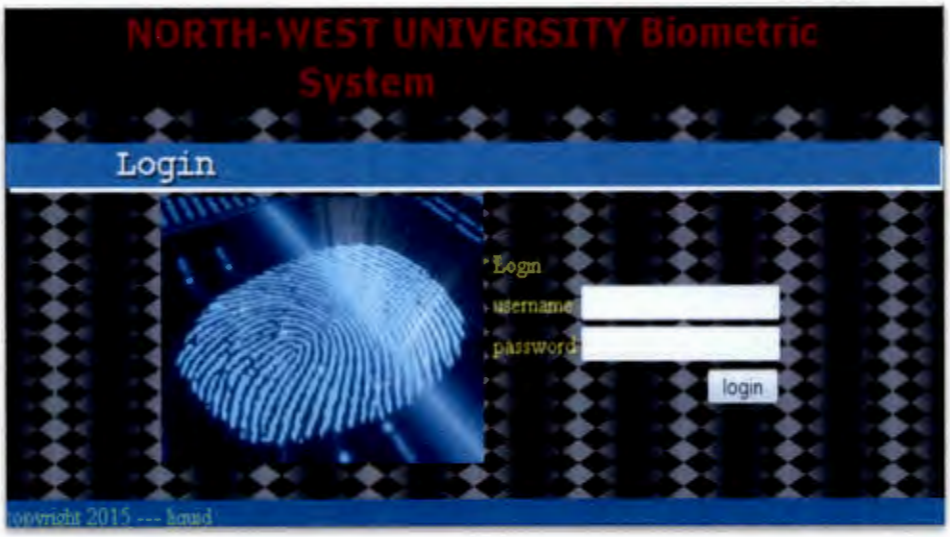

Figure 6.8: The Login Screen

The interface shown in Figure 6.7 above represents the scanner at the gate. It displays the view of the very first screen that the system users see when they visit the web based component of the biometrics system. After authentication each user is directed to their respective interfaces.

6.7 System Administrator Interface

The interfaces shown in Figure 6.8 and 6.9 respectively, represents the account creation and accounts list interfaces respectively. These interfaces belong to the system administrator. Figure 6.8 displays a form that is used to capture user details then it is submitted using a PHP script to a MySQL database. Figure 6.9 represents the account creation form which is the output /results from the account creation form. It is displayed by running PHP embedded Sql commands. The outcome is then given in the list shown in Figure 6.9.

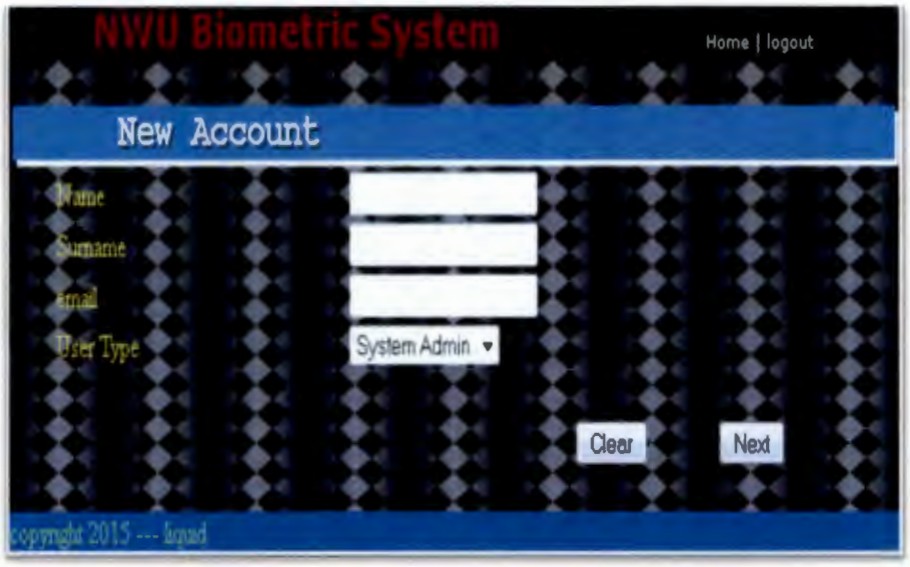

Figure 6.9: Account Creation Form

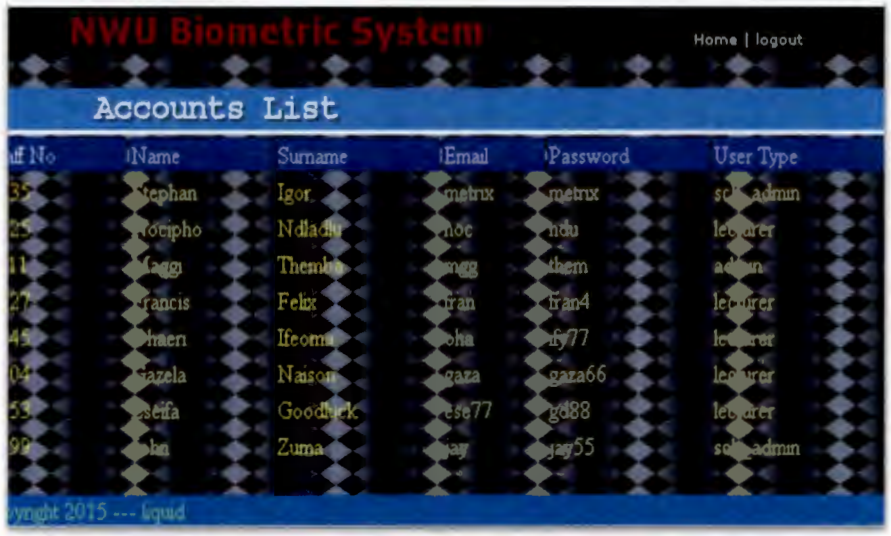

Figure 6.10: Accounts List

6.8 School Administrator Interface

The interfaces shown in Figure 6.10 is used to collect student information to be stored in the database; while the interface shown in Figure 6.11 below that is a sort of feedback that follows suite which indicates what modules the student has just registered for.

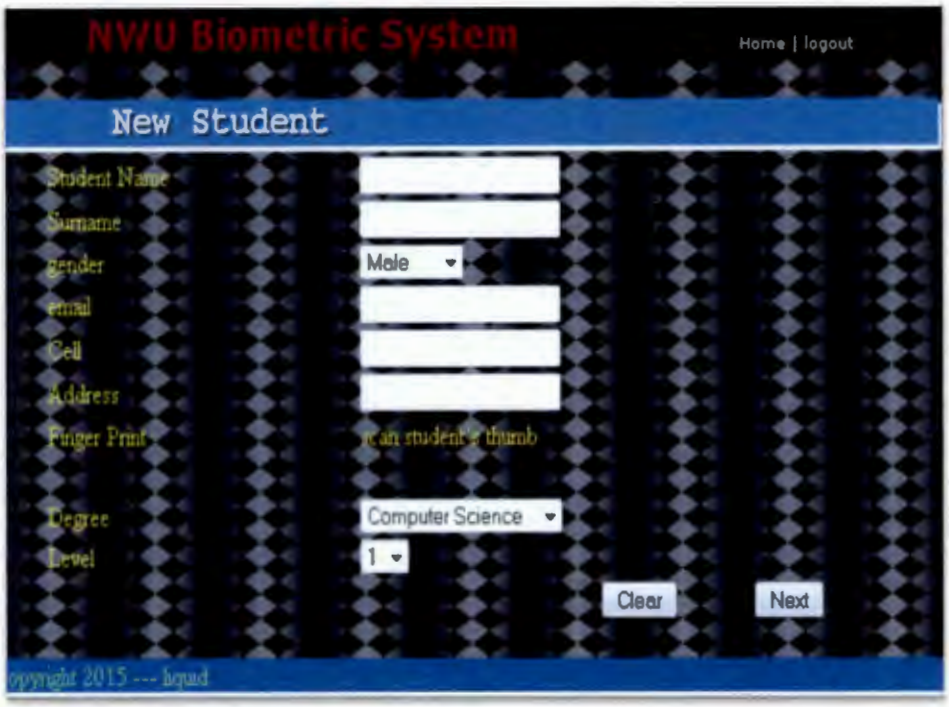

Figure 6.11: Students Registration Form

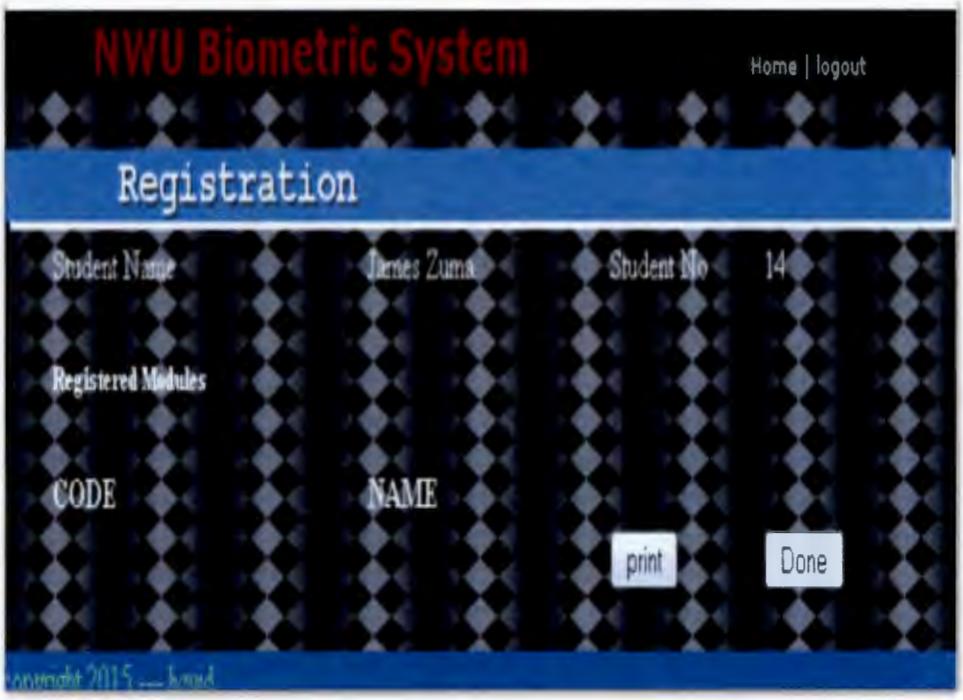

Figure 6.12: Proof of Registration

The interface in Figure 6.12 is displayed when the administrators request for a list of registered students the table below is generated and then displayed.

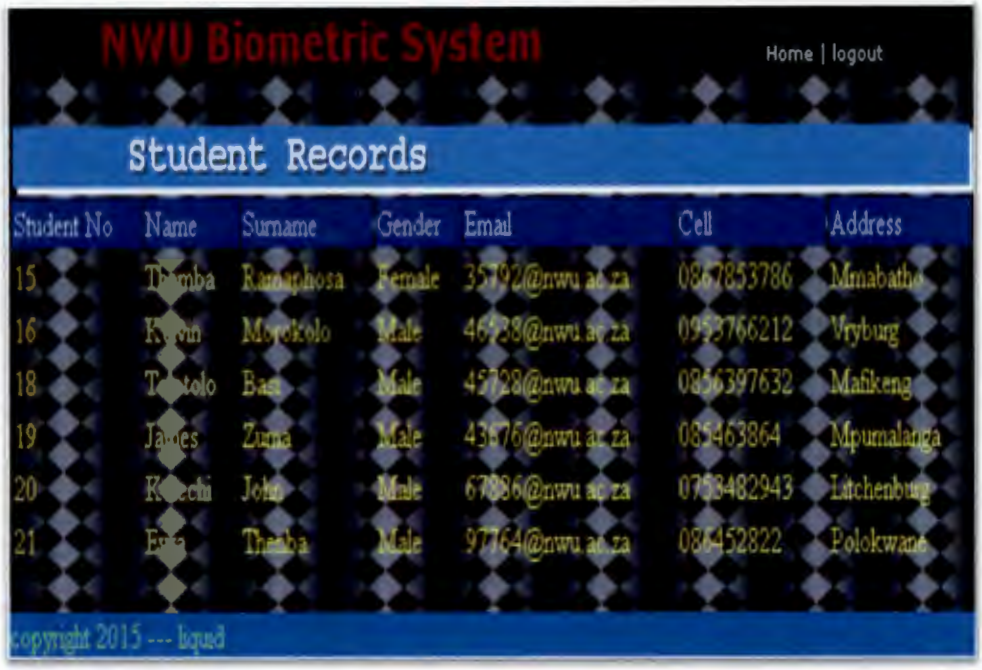

Figure 6.13: List of Registered Students

The interface shown in the Figure 6.13 is the interface form for creating a new module.

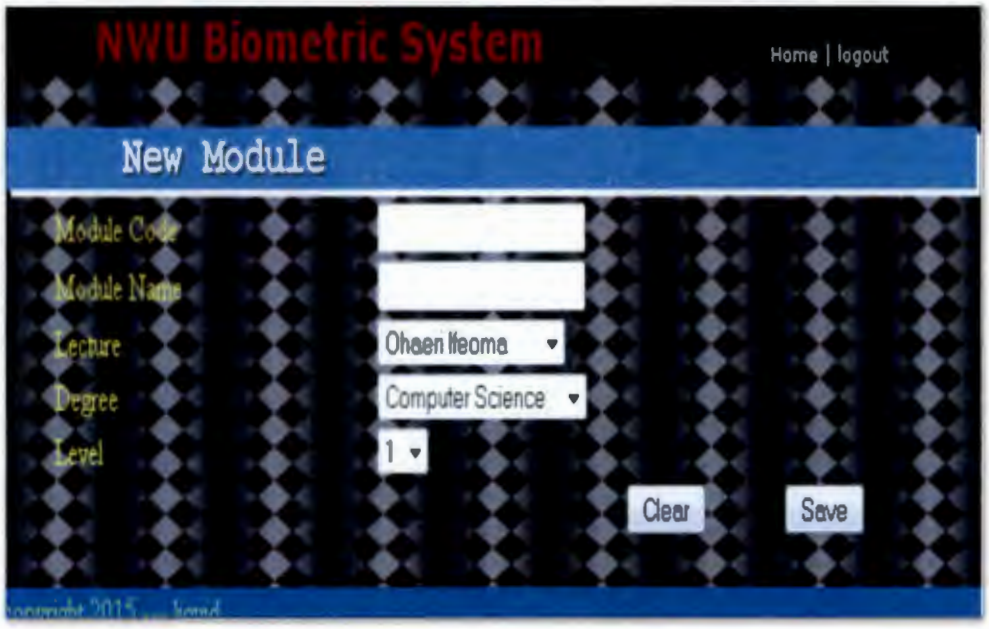

Figure 6.14: New Module Form

It is a form used to insert module information. Note that the lecture field and degree fields are select menus; these are extracted from the database to restrict the user to make valid options. The save button is used to save the form data into a MYSQL database.

However, on retrieval, the list of modules is displayed as show in Figure 6.14.

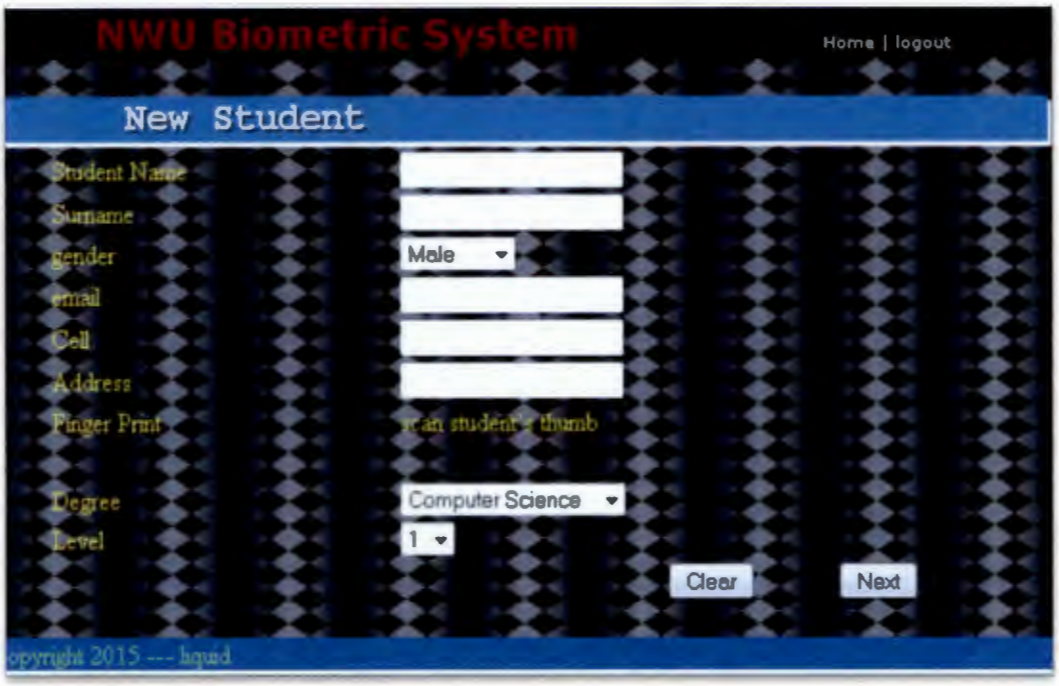

Figure 6.15: List of Modules

The administrator is also responsible for creating the time table for each venue. The Figure displayed in the Figure below shows the time slot creation form. It has in it the name of the venue, the module, the date and the duration – the start time and the finishing time.

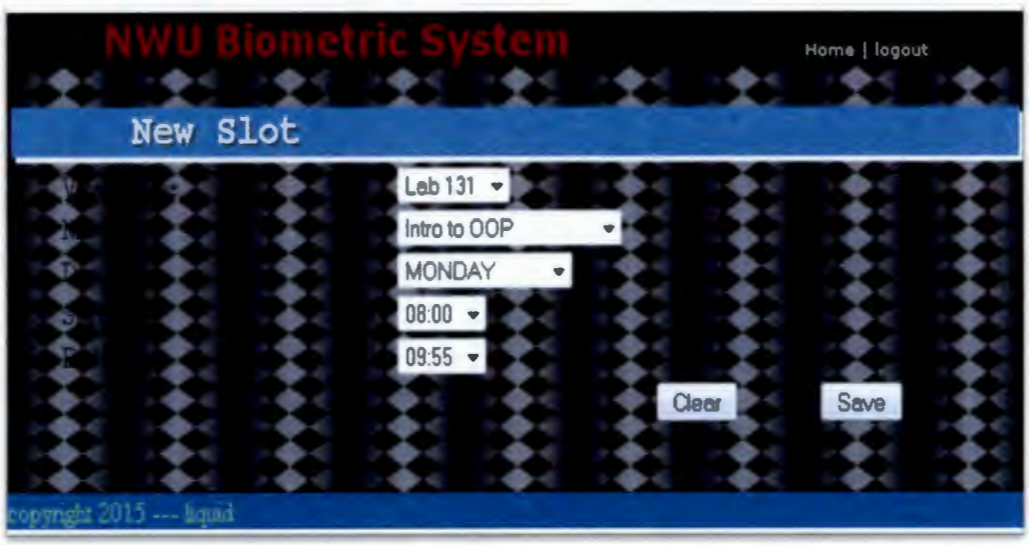

Figure 6.16: New Time slot Form

The user is restricted to predetermined set of inputs by using select menus to avoid input errors. After the data has been entered it can be viewed, if requested the list is displayed in a PHP table as shown in Figure 6.16.

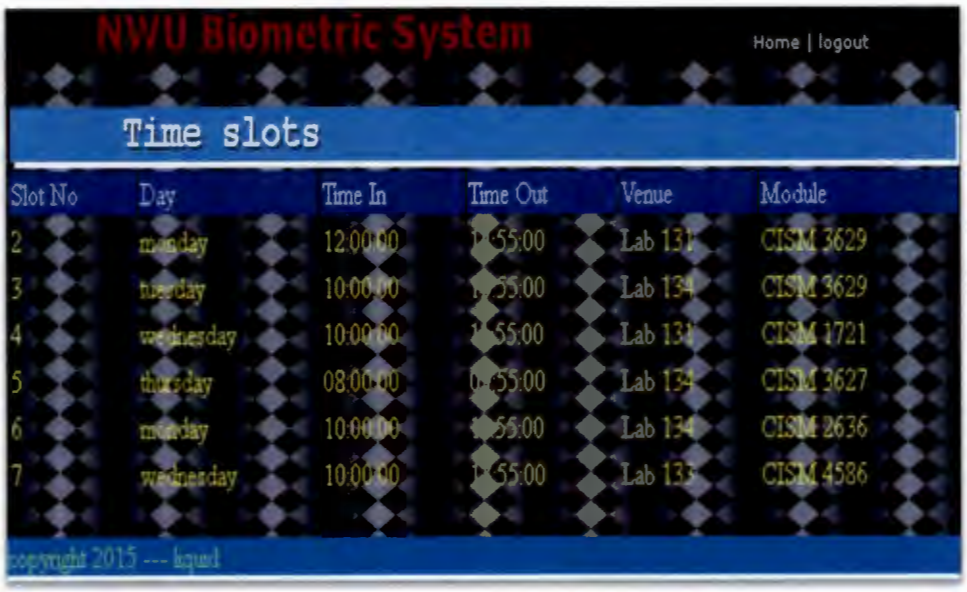

Figure 6.17: Time Slots

6.9 Lecturer Interface

As previously stated when each student gains entry to any venue an attendance list is automatically generated in the background by the system. The system records the student`s details and the time entry was made. After class the lecturer can log in and view the attendance register.

The window is shown in the Figure 6.17.

Figure 6.17: Attendance Register

The lecturer selects a module from a select menu that contains all modules that he/she lectures. He/she than loads the dates, the dates list will contain all dates that the particular module was attended then on clicking submit an attendance register is generated.

All the interfaces presented above have a small navigation bar at the top right. The bar contains Home and logout. The home link sends the user to their home page while the logout link cancels the session thus the user is locked out of the system and is sent to the login screen.

6.10 Impacts/Benefits of Biometric System

If the biometrics system designed in this thesis can be properly deployed in real time by the university for access control to physical locations such as; laboratories, buildings, lecture venues gates etc., it can effectively record the students' attendance, monitor the rate at which the laboratories are being used and also keep records of who enters the premises and at what time. Obviously, this will make the traditional methods of taking manual attendance registers and using cards at the entrances obsolete because they are inefficient in terms of adequate security and proper identification in cases of serious crimes and robbery. Typically, the use of fingerprint authentication, and identification system improves access control into physical locations such as; buildings, laboratories, lecture venues, and logical information - personal computer accounts, electronic documents, and so forth.

However, this thesis supports that under a reliable, effective and efficient authentication and identification system, digital forensics can function effectively. Should criminal and fraudulent cases occur, of which they are unavoidable among large institutions such as the higher institutions it would be easier to trace. This is because everyone who is part and parcel of the university has his/her fingerprint biometrics already stored in the database and every new participant is also captured at every entrance and also stored in the database such that it is constantly automatically updated. Here, NWU was used to demonstrate the functionality and areas of applicability of using the biometrics identification.

Moreover, the benefits of BT are quite numerous when compared to other mechanisms for verification/authentication or identification in several ways listed below:

i. Tokens, PINs, passwords, shared secrets, and numbers are proxies for the individuals that hold them. Systems that recognize these are attempting to recognize individuals indirectly, whereas biometrics uses the body as a proxy for the individual.
ii. The non-biometrics verifiers must match exactly. Because there is no permissible "within class" variability, "close enough" is not considered. A PIN is not correct unless all the digits match. Passwords generally require that the user type with the

correct case. On the other hand, an individual cannot precisely re- peat biometric verifiers because of changes in biology, behaviour, and the collection environment

iii. If security for the parties involved in an application depends on non-transference of authorizations, non-biometric verifiers are not as secure as biometric characteristics, which are more difficult, although not impossible, to give to another person.

iv. PINs, passwords, shared secrets, and numbers can be assigned to fictional persons, legal persons, and agents, allowing for actions on behalf of natural individuals. I can give my spouse my ATM card and PIN for bank deposits and withdrawals on my behalf, but not my iris pattern.

v. System management knows and can control how much fundamental "between-class" variation exists between PIN or password verifiers, by using long string length or assigned PINs, for instance. The fundamental variation in observed biometric verifiers across different populations and observation environments is not well understood.

vi. System administrators can revoke or reissue tokens, PINs, and passwords. System policy might require the user to choose a new PIN every 60 days, for example, while biometrics characteristics are fixed to the data subject.

vii. Tokens, PINs, and passwords can be application specific; biometrics characteristics cannot be application specific. Every application that requires my right thumbprint has access to that verifier. As verifiers, biometrics attributes have very different qualities and thus are not transparently interchangeable with PINs, passwords, keys, and tokens. Each method has a different impact on security, privacy and usability.

These applications promote privacy and security because only the account holder can access the digital records. They also promote convenience to the extent that placing a fingerprint on a scanner is faster than the alternatives.

6.11 Biometrics System Capability and Evaluation Criteria

Having implemented the biometrics system and analysed the results obtained, it is imperative to evaluate the analysis based on the fundamental biometrics system security objectives and capability measures.

Oftentimes, business processes and transactions are affected as a result of forgotten passwords and lost identification cards. For example, forgotten passwords result in helpdesk calls and replacements which are expensive to businesses and clients. It is now widely

documented that fingerprint systems can significantly reduce the spending on helpdesk calls and assistances much beyond the cost of investment. The use of fingerprint systems facilitates businesses to move to an automated, user-friendly, self-service support model while providing the same or even higher level of security as the attended model. This thus lessens the business's expenses.

Also in applications with a negative claim of identity, such as background check, for instance, in "security clearance", voters" registration, and multiple enrolments checks, duplicate passport, and driver license checks, there are no alternatives to biometrics. Fingerprint authentication/identification systems, when properly implemented; provides more security, convenience and efficiency than any other means of identification.

No other technology has the capability to guarantee non-repudiation and ensures that the individual being authenticated is physically present at the point of authentication/ identification. Fingerprint-based authentication systems have replaced passwords and tokens in a large number of applications. Though in some other applications, they are used to add a layer of security on top of passwords and tokens. The use of fingerprint authentication systems will increasingly reduce identity theft and fraud and ensure privacy. As fingerprint recognition technology continues to advance, an increase erupts in the interaction among markets, technologies, and applications. This emerging interaction is expected to be influenced by the added value of the technology, the spontaneous responses of the user population, and the credibility of the service providers. We cannot categorically predict now where and how fingerprint technology would evolve and transcend to and be mated with its applications, but it is certain that fingerprint based authentication systems will have a profound influence on the way businesses are conducted on a daily basis [53 , 87].

In spite of these promises which biometrics system offers, its rate of deployment still encounters several barriers and limitations which are discussed below.

6.12 Barriers of Biometric System Deployment

A fingerprint recognition system provides a good balance of security, privacy, convenience, and accountability. While the adoption of these systems is steadily increasing, the rate of adoption has been somewhat slower than anticipated. This is primarily because of a lack of awareness of the benefits and capabilities of fingerprint technologies. Another reason is that

the business perspective on fingerprint recognition systems (return on investment analysis) has often proven to be somewhat difficult due to the following reasons:

- The business value of "security" and "deterrence" is difficult to quantify in terms of return on investment, regardless of the technology.
- Fraud rates and the resulting cost of long standing business and government systems (for example, tokens and passwords) are not well understood and quantified.
- Fingerprint recognition systems, being emerging technologies, are sometimes confronted with unrealistic performance expectations and not fairly compared with existing alternatives (for example, tokens and passwords), whose inconvenience and high costs businesses have resigned to tolerate. A successful fingerprint-based solution does not have to be perfect in terms of accuracy and fool-proof in terms of security. A particular application simply demands a satisfactory performance justifying the additional investments needed for the fingerprint system. The system designer can exploit the application context to engineer the system to achieve the target performance levels at an acceptable cost.
- The "quality" of available fingerprint technology varies quite considerably from one application to another and from one vendor to another. Businesses cannot often easily access credible reports on technology evaluations because of a dearth of standardized scenario testing of fingerprint systems. This leaves businesses to either perform their own evaluation (which delays deployment) or rely on references (which could be difficult to obtain because of unique operational scenarios).
- Several fingerprint system vendors are not financially stable, leaving businesses with concerns over continued product and support availability [87, 79].

Based on these barriers and limitations the system is prone to vulnerabilities and threats.

6.13 Biometric System Vulnerabilities and Threats

Biometrics systems' positive aspects are widely appreciated within the technical community, but fear of their negatives drives many away. The certainty of vulnerability to attacks still exists. However, eight specific locations have been identified as being the most vulnerable positions in a biometrics authentication system. The diagram shown in Figure 5.18 indicates the possible attack locations in the system [138]. We have discussed them categorically below.

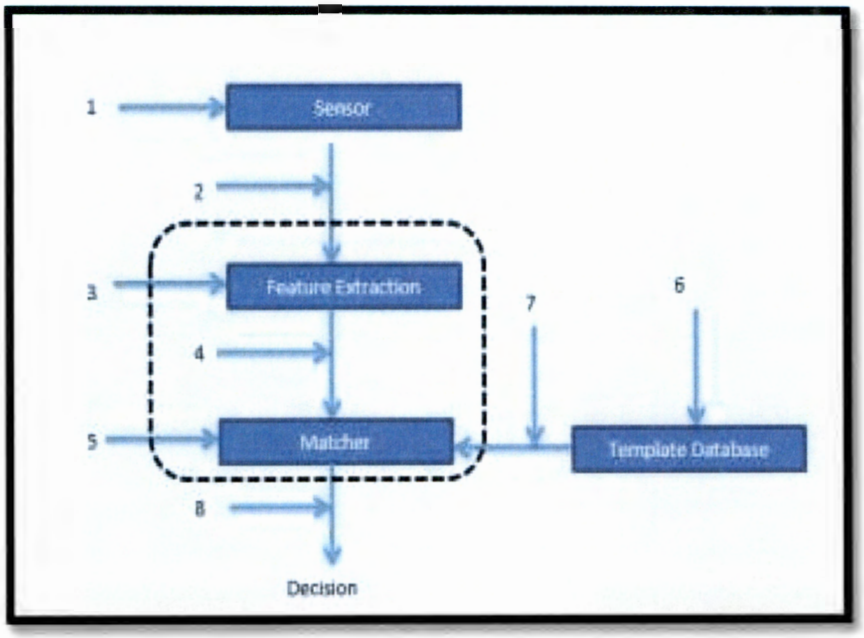

Figure 6.18: Attack locations in a Biometric Authentication System [138]

Type 1: Attack where a non-user would present a fake biometrics, this clearly shows that in as much as biometrics systems are reliable their templates are also exposed to being duplicated.

Type 2: Is submitting a previously cut-off biometrics sample; it can be from a previously enrolled user who still has access to the system.

Type 3: The attacker can also temper with the feature extraction module to produce feature values that match the ones in the template.

Type 4: In addition to type 3 attack, the attacker can replace genuine feature values.

Type 5: The attacker can also be able to modify the matcher such that it outputs an artificially high matching score.

Type 6: Are attacks that can happen on the template itself, for instance modifying the current template or changing the template all together.

Type 7: The transmission medium is also prone to attacks; these are medium between the template and the matcher. Lastly,

Type 8: Occurs when the matcher results are overridden by the attacker. These forms of attacks are also classified as direct and indirect attacks. Where direct attacks are the ones that take place at the sensor level, no knowledge of the system is needed concerning the attack. Indirect attacks are the rest of the seven areas of the biometric authentication system.

Furthermore, certain threats are also associated with generic authentication application [139].

A. Denial of Service: In denial of service (DoS) this is where an attacker corrupts the authentication system so that legitimate users do not gain access, an example of DoS would be when an online server is attacked with a lot of bogus access request to a point where the server's computational resources cannot handle valid requests any more.
B. Circumvention: In circumvention the attacker gains access to the system protected by the authentication application, this occurs when attacker access information that he was never authorized for. In repudiation the attacker denies accessing the system, an authorized user may claim that his biometric data was stolen after modifying the records illegally.
C. Contamination: In contamination an attacker obtains a biometrics data of a legitimate user and uses it to access the system that is the biometrics data associated with a specific application can be used on another different system. In collusion a legitimate user with wide access privileges is the attacker who illegally modifies the system; an example would be the administrator of the system being the attacker. In coercion an attacker forces the illegitimate user to access the system, the situation occurs when an attacker use the fingerprint of an authorized user forcefully to access the data [138]
D. Trojan horse: In attack 3 – (feature extractor) and 5 - matcher, a Trojan horse might be used in order to carry out the attack; this can bypass the feature extractor and the matcher correspondingly.
E. Modification, Deletion / Add: In attack 6 the imposter is capable of modifying, deleting or adding to the system's template. The attack is directed to the system's database. Finally, the remaining attacks exploit possible weak points in the communication channels regarding the system, i.e. extracting, adding and modifying information from the communication channels [139]

Therefore, it is evident that although biometrics authentication systems are justified to be unique in identifying an individual, they are also vulnerable to a lot of attacks and threats [140]. Hence, digital forensic mechanisms should be put in place to further identify impostors should the system be involved in any serious crime.

6.14 Chapter Summary

In this chapter we have provided the practical aspect of biometrics technology that forms the security infrastructure to enhance information security and network management. The chapter demonstrates how the system is implemented by transforming some of the artefacts from the requirements analysis reported in chapter 3 and earlier in this chapter. The biometrics authentication system operates using NWU biometric system as its application domain for implementation. Consequently, this research project presents the deployment of biometrics systems as a reliable security mechanism to enhance information security and network management by effectively monitoring security breaches and enabling digital forensic technology whenever necessary.

Therefore, it is evident that although biometrics authentication systems are justified to be unique in identifying an individual, they are also vulnerable to a lot of attacks and threats [140]. Hence, digital forensic mechanisms should be put in place to further identify impostors should the system be involved in any serious crime.

Chapter 7

Summary, Conclusions and Future Work

7.1 Summary

Summarily, this study on digital forensic and biometrics analysis for information security and network management was reported in two sections namely; Biometric Analysis Section and Digital Forensic Analysis Section as we earlier stated. There has to be a system upon which we can measure crime and then suggest a mechanism to combat the crime. This study was very crucial at this point in time to measure the current level of technology and understand where it is going. Information within the context of this research can be said to be data that is accurate and timely, specific and put together on a subject for a defined purpose. Information presented carefully within a context can produce relevance. It is valuable because it can affect behaviour, a decision, or an outcome. How it is handled can also lead to an increase in output and decrease in uncertainty. Therefore, information is a very sensitive asset and should be handled with a sense of control and knowledge so as to avoid loss of an advantage or level of security if misappropriated. Hence, there should be a practice of securing and protecting information against non-authorized use and access, disruption and, disclosure, modification and inspection, perusal and destruction and recording, irrespective of the manner it is being used. We can categorically say that information cannot exist without a system. Information systems house information and jointly connected to form a network. Thus, having no adequate security over a system or a network is like building a mansion, well furnished with expensive furniture and interiors without putting a security system on the door and one travels far. Definitely, the contents of the house are likely to be stolen. Moreover, information and network management as a component of any system monitors and controls the system objects and allocates its resources in the information base (IB). It is defined by a management policy and maintained by a device/structure. Therefore deploying efficient, effective and reliable security infrastructure for its adequate functionality should be our uppermost and deepest concern. Information and network management systems play important roles not only in the organizations, companies, or institutions but in our everyday lives. Hence, they need to be adequately secured / protected. Therefore, the study on Digital Forensic and Biometric Analysis for Information Security and Network Management conducted here was quite relevant and timely because every institution, company and organizations that uses

information, its systems, and networks requires an adequate security infrastructure to be stable and operational.

Digital forensic technology is very important because most impostors are becoming knowledgeable on steganography and encryption methods that are used for hiding data and digital evidence beyond the capability of the traditional searching methods. Indeed there is so much to forensic processes than what we can literally imagine. Not only that they offer detective and discovery techniques, they also involve various activities that assure the security and proper handling of fragile information, such that it does not get damaged or corrupted along the process of investigation. Because the data integrity must be justified while keeping the rules and laws of digital evidence that guarantee admissibility in court. Hence, we have designed a model for a digital forensic process that justifies the goal of this thesis. We achieved this from the already existing knowledge in literature and the model was presented in a methodological manner and properly applied, it will enhance information security and network management.

Moreover, biometrics technology has been extensively reported as a method of security control and management, and significant effort is reported in this thesis by implementing fingerprint verification/authentication system in the institution for effective monitoring of attendance especially at NWU which we used as the application domain.

7.2 Conclusion

Crime is both a local and a global phenomenon; the criminal activities are increasing rapidly so the science to tackle them should be equally growing globally at the same rate in order to sustain the forever advancing technology and its consumer community.

This study on digital forensic and biometrics analysis as reported in this thesis was conducted in order to ascertain their uniqueness and effectiveness in providing adequate, reliable, and effective security via digital forensics and biometrics systems. Our biometric analysis reported in this thesis draws on patterns and measurements of fingerprint extraction and authentication system in other to enhance information security and network management. Forensic experts perform analyses that depend largely on their individual knowledge, previous experience and judgement through the methodologies reported from our designed model and some of the tools described in this treatise.

We have highlighted and discussed the essential components in our digital forensic process model being preparation/ extraction, examination, and analysis. They tend to establish facts using evidence and in order to identify a culprit/criminal/impostor.

This study on digital forensic analysis focused mainly on the discussion on our digital forensic process model towards enhancing information security and network management. The main aim of implementing biometrics technology is basically for a better identification and also a verification process that is much more convenient and accurate. This has been emphasized in this study.

Analytically, the architectural design, flowchart and model have effectively been used and presented as a part of the system development. The essence was to systematically analyse the various phases, stages, and sections involved in the digital forensic and biometrics technology analysis and the biometrics authentication system which results in digital forensic processes/procedures. They described the procedures structurally in order to enable system configuration. Consequently, a high confidence and affordable biometrics, especially fingerprint authentication systems, have emerged as the mainstream of security solutions. As reliance on biometrics technology increases, there is a possibility of it becoming a standalone technique for determining individual's identity, which obviously eliminates the carrying of cards around and the need to remember passwords Categorically, biometrics authentication identifiers the user based on biological features and digital forensic may detect an impostor via its biometrics characteristics that are extracted from a crime scene. Digital forensic and biometrics analysis enhance information security and network management. This is the main goal of this thesis. This we have achieved by providing answers to the research questions and their corresponding research objectives.

Firstly, we presented the requirement analysis and design of biometrics and digital forensic (BDF) analysis concepts such as: architecture, model, and flowchart which are specific to biometrics and digital forensic analysis for information security and network management. It specifically responded to the research question 1 and its corresponding research objective.

The algorithms of fingerprint image processing with its implementation in MATLAB and the corresponding results were also presented. It generally provides the underlying sequence in the generation of fingerprint minutiae which are stored on the database of fingerprint

authentication and identification systems designed in chapter 4. It specifically gave response to the research question 2 and its corresponding research objectives.

Thirdly, we reported the basic requirements necessary for the development of a fingerprint biometrics authentication (FBA) system which can be deployed at lecture halls to monitor students' attendance. Following the basic requirements, an FBA system was designed, implemented and also, reported the results as proof of concept to validate the thesis idea. It specifically gave response to the research questions 2 and 3 and their corresponding research objectives. The designed FBA can effectively record the students' attendance to lectures when deployed at the entrance to lecture venues. This system requires that all the students be registered for their modules using their fingerprint. Then at the entrance to the lecture venues and other recommended areas, the samples of their fingerprints can be captured using the device located at the entrances. The system takes the attendance at both the beginning and at the end of the lectures to ensure that the students were present throughout the entire duration. Also, we discussed all the interfaces indicating the design, implementation, and result analysis phases such as: System Requirements, Use Case Descriptions, Activity Diagrams, Database Design, and the System Interfaces.

However, the approach shows that, for us to succeed in building a bridge between the DFT and BT a system that initially captures and stores the biometrics trait must be deployed. This is because authentication and identification cannot exist without referring to an already existing sample in the database for matching or comparison. This will aid DFT when it is necessary to be deployed for identification of a perpetrator and reporting in court. Otherwise, it will be difficult though not impossible for DFT to be utilized in such identification. Therefore, we recommend that all institutions, organizations, and companies deploy biometrics technology authentication for easy deployment of DFT. However, the approach shows that, for us to succeed in building a bridge between the DFT and BT a system that initially captures and stores the biometrics trait must be deployed. This is because authentication and identification cannot exist without referring to an already existing sample in the database for matching or comparison. This will aid DFT when it is necessary to be deployed for identification of a perpetrator and reporting in court. More so, system capability and deployment, system impacts/benefits system vulnerabilities, and threats are also reported in this chapter.

Lastly, we designed and described the digital forensic analysis process model in this thesis. It analyses the phases involved in digital forensic analysis methodologically. It also includes the priority of digital forensic towards the deployment of fingerprint (biometrics) technology for improving and enhancing information security and network management

In order to justify the goal of the thesis, we conducted experiments and logical analyses based on our methodology. From the results obtained, we made the following findings:

i. Biometric Technology can be used to determine whether or not someone exists in any applicable database.
ii. Biometric Technology can also be implemented anywhere where there is a need to recognise and identify an individual.
iii. Biometric applications can be useful in several other collection environments where accountability monitoring or applications are required which include identification when boarding an air craft, signing a document, for an equipment collection or recording the chain of evidence.
iv. Biometric authentication and identification systems are more reliable when engaged in a restricted area like laboratories and offices.
v. Biometric authentication can be applicable wherever there is a need to confirm if a person has the privilege to perform certain activities in a network or system while, identification is applicable wherever the need arises to determine if someone is in a database or not without necessarily a claim of identity.
vi. Digital forensic Technology can be applied on biometric systems. Expressed in this thesis is the fact that Deleted data from the user's point of view can be recovered even when deleted using techniques for recovery of deleted data/information. This component constitutes the central focus of digital forensics which states that data stored digitally can be manipulated; therefore, adequate security is required for every functional network and system. Digital evidence must be handled with much care at all stages of the investigation process such that; the origin/source of the evidence can be proved or defended.

Based on the above findings we provide a few recommendations:

A. Evaluation of various biometrics features can be conducted to measure their relative performances.

B. Digital forensic investigation can be conducted in real time environment relating to some biometric features using specified digital forensic tools.

7.3 Future Work

Information, systems and networks are key technologies for several applications but having them adequately secured is a critical requirement that can never be overemphasized. Yet, there is a significant lack of reliable, efficient and effective security mechanisms that can be easily implemented. It is important to note that any information system and network can never be totally and completely secured. This is because as technology advances on a daily basis, attacks replicate and attackers' tools also gets sophisticated on a daily basis. This makes 100% security not realizable irrespective of the security mechanism deployed. Basically, a reliable, efficient and effective security mechanism properly put in place helps in reducing the attacks to a minimum.

Therefore, system analysts and security administrators must act as watch dogs over the systems and networks to ensure that attacks and intrusions are drastically reduced to their barest minimum by overhauling and upgrading the security systems regularly. Biometric information offers a reliable and secure solution to the problem of user identification but, is vulnerable to a number of attacks and threats. Securing information systems and networks can be applicable to securing biometrics information by encrypting the biometric identification information and the entire communication channel. There is no biometrics template protection mechanisms sufficiently effective in enabling adequate protection of biometric templates used in high recognition performance systems. This public perception and the system security concerns have been the main barriers to its deployment. For this reason, we intend to take this research another step forward to the "Analysis of Cryptography and Steganography Implementation for Biometric Systems". Encryption is one of the techniques that can secure biometrics; basically it requires: (i). the design of a cryptographic and a steganography algorithm, and (ii). the implementation by running both algorithms at the transmission rates of the communication links over the network.

Consequently, security of networks is not about seeing computers at both ends of a communication channel, but it also ensures that communication channels are not prone to attack because a hacker/attacker can target an uncovered biometric image and encrypt it and send false message that is capable of harming and keeping the network under hostage.

Therefore, enhancing information security and network management principles discussed in this thesis can in the future be extended to - Analysis, Design and Implementation of Cryptography and Steganography Algorithms for Information Security and Network Management on the aspect of biometrics technology and Analysis of real-time Implementation of Digital Forensic Technology using a specified Tool.

References

[1] D. Mellado, E. Fernández Medina, "A Common Criteria Based Security Requirements Engineering Process for the Development of Secure Information Systems." International Journal of *Computer Standards and Interfaces,* vol. 29 (2), pp. 244 - 253, 2007.

[2] L. E Sánchez, A. S.O. Parra, "Managing Security and its Maturity in Small and Mediumsized Enterprises, "*Journal of Universal Computer Science*, vol. 15 (15), 3038 – 3058, 2009.

[3] A. L. Opdahl, and G. Sindre "Experimental comparison of attack trees and misuse cases for security threat identification." Information and Software Technology. In Press, Corrected Proof, 2008.

[4] P. Hunton. "The stages of cybercrime investigations: Bridging the Gap between Technology Examination and Law Inforcement Investigation," *Computer Law and Security Review*, pp. 61-67, 2011.

[5] Z. Xiu-yu. "A Model of Online Attack Detection for Computer Forensics. *IEEE International Conference on Computer Application and System Modeling*, 2010, pp.533-537.

[6] W. V. Staden, and M. S. Olivier. "On Compound Purposes and Compound Reasons for Enabling Privacy." *Journal of Universal Computer Science*, vol. 17 (3), pp. 426-450, 2011.

[7] A. Sabah, and A. Bashayer. "Modeling the Forensic Process" *International Journal of Security and Its Applications,* vol. 4, pp. 98-108, October, 2012.

[8] G. Pangalos, C. Linoudis, and I. Pagkalos." The Importance of Cooperate Forensic Readiness in the Information Security Framework," in *Proceedings of the IEEE Workshop on Enabling Technologies infrastructure for Collaborative Enterprise"* 2010, pp.12-18.

[9] B. D. Carrier, and E.H. Spafford," An Event-Based Digital Forensic Investigation Framework," in *Proceedings of the Digital Forensic Research Workshop*, 2004, pp.1-12.

[10] D. Kim, K. Chung, and K. Hong. "Person Authentication using face, teeth, and print recognition on mobile phones" *EURASIP Journals on Signal Process*, vol. 10,January 2008

[11] A. Martin, C. L. Wilson, and M. Przybocki, "An Introduction to Evaluating Biometric Systems," *IEEE publication for National Institute of Standard and Technology*, pp. 158-156, 2000.

[12] N. S. Yogendra, and S.S.Kumar. "Vitality Detection from Biometrics: State of the Art. *IEEE Publications,* vol 5, pp. 225- 228, 2011

[13] L. Simson, and V. Garfinkel. "Digital Forensic Research: The next ten years." *Elsevier publications,* pp. 64-69, 2010.

[14] J. Yang, and T. Li. "Computer Forensics System Based on Artificial Immune Systems."*Journal of Universal Computer Science,* vol. 13, pp. 139-142, 2007.

[15] G. Francia, and K. Clinton. "Computer forensics laboratory and tools." *Journal of Computing Sciences in Colleges* ,vol. 25, 143-150, 2006.

[16] K. Nance, and M. Bishop. "Introduction to Digital Forensics - Education, Research and Practice Mini track", *in proceedings of the IEEE 45th Hawaii International Conference on System Sciences,*2012, pp. 5022-5025.

[17] M. A. Reis, and G. P. L. "Standardization of Computer Forensic Protocols and Procedures", in *Proceedings of the 14th First Conference on Computer Security Incident Handling & Response.* 2000, pp. 15-20.

[18] C. Bashaw. "Computer Forensics in Today's Investigative Process", in *proceedings of the 15th first Conference on Computer Security Incident Handling & Response*, Ottawa, 003, pp.523-527.

[19] M. Srinivas and A. H. Sung. "Identifying Significant Features for Network Forensic Analysis Using Artificial Intelligent Techniques." *International Journal of Digital Evidence,* vol. 1, pp. 500-505, 2003.

[20] J., M. "Computer Forensics in a Global Company", in *proceedings of 16th International Conference on Computer Security Incident Handling & Response.* Budapest, 2004, pp.109-117.

[21] F. Lan. "A Framework for Network Security Situation Awareness Based on Knowledge discovery", in *Proceeding of the IEEE 2nd International Conference on Computer Engineering and Technology*, 2010, pp. 226-231.

[22] M. Gerber, and S. Rossouw von. "Information security requirements – Interpreting the legal aspects, "The Elsevier Publication in Computers & Security, vol. 27, Issues 5–6, pp. 124– 135, October 2008.

[23] J. Slay, and A. Koronios. *Information Technology, Security and Risk Management.* 44 Casmire. Australia: John Willy and Sons Company, 2006, pp. 560-580.

[24] T. Benson, R. Kennerer, and B. Lampson. "Information Systems Security: Fundamental Challenges" *National Academy Press*, pp. 105- 110, 1999.

[25] B. Unauméés, and S. A. A. Zeidler. "Enabling Personal Privacy for Pervasive Computing Environments." *International Journal of Universal Computer Science*, vol. 16, pp. 341-371, 2010.

[26] B. Fal, A. M. "Standardization in information security management" *Journal of Cybernetics and Systems Analysis*, vol. 46, 181-184, 2010.

[27] H. Jerome, V. Saltzer, and M. Frans Kaashoek "Principles of Computer System Design: An Introduction" *Massachusetts Institute of Technology publication*, pp.1-9, June 24, 2009.

[28] A. Edward Robert. "Security and Privacy Controls for Federal Information Systems and Organizations". *National Institute of Standards and Technology Publication*, pp.800-806, 2011.

[29] X. Weiguan, W.Houkui, and H. Haoyi, .Donghong. "The Analysis of University Network Information Security System Based on Level Protection Model", in *Proceedings of the eight International Conference on computational Intelligence and Security,* 2012, pp.609-614.

[30] C. Wooi, C. Liu, and G. Manimaram, "Vulnerability Assessment of Cyber Security for SCADA Systems". *IEEE Journal on power systems*, vol. 23, pp.1836-1846, November, 2008.

[31] S. Berinato, "A Few Good Information Security Metrics." *CSO Magazine*, pp. 556-260, 2005.

[32] N. F. Doherty, and H. Fulford "Aligning the Information Security Policy with the Strategic Information Systems Plan." *Journal of Computers & Security,* vol. 25(2):vol. 10, pp. 55-63, 2006.

[33] Jansen, W. and T. Grance. "Guidelines on Security and Privacy in Public Cloud Computing." *NIST Special Publication*, pp. 100-144, 2011.

[34] N. Mastali, and J. Agbinya. "Authentication of Subjects and Devices Using Biometrics and Identity Management Systems for Persuasive Mobile Computing: A Survey Paper". *Journal of Information Technology and Security*, vol. 5, pp. 256-262, 2010.

[35] W. Wei, and L. Sun. "Innovation Teaching and Learning Experiences in Network Attacks and Defence", in *Proceedings of the eight International conference on Computational Intelligence and Security,* 2012, pp. 587-590

[36] R. S George Weir. "Issues and Perspectives", in *Proceedings of the first International Conference on Cybercrime, Security, and Forensics,*" 2011, pp. 720-728.

[37] G. Pangolos, C. Ilioudis, I. Paglalos."The Importance of Corporate Forensic Readiness in the Information Security Framework", in *Proceedings of IEEE 2010 workshop on Enabling Technologies: Infrastructure for Collaborative Enterprise*, 2010, pp.12-16.

[38] Park, C.-S., S.-S. Jang. "A Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance". *IJCSNS International Journal of Computer Science and Network Security* vol. 10(3), pp. 10-21, 2010.

[39] W. Sabrina, S.Tjoa, H.Zahoa, and K. Liu. "Digital Image Source Coder Forensics via Intrinsic Finger Prints", *IEEE Journal on transactions on Information Forensic and Security*", vol.4, pp. 460-475, September, 2009.

[40] J. Zhang, L. Wang."Integrated Open Source Forensic Environment for Digital Evidence Investigation", *Wuhan University Journal of Natural Science*, vol. 17, pp. 511-515, 2012.

[41] H. Gua, B. Jin, W, Qian. "Analysis of Email Header for Forensics Purpose", in *Proceedings of IEEE, 2013 International Conference on Communication Systems and Network Technologies*, 2013, pp.340-344.

[42] D.O Report, "Department of Defense Cyberspace Policy Report". *Pursuant to Section 934 of the NDAA of FY,* pp. 1-30, 2011.

[43] N. S. Sargur, C. Huang, S. Harish, V. Shah. "Biometric and Forensic Aspects of Digital Document Processing," 2010, pp. 720-728.

[44] T. Killion," Biometric Identity Management" in *Proceedings of the International Conference on Biometric*, 2011, pp. 2250-2260.

[45] S. H. Van Solm, and C. P Lourens. " A Control Framework for Digital Forensics" International *Journal of Digital Evidence,* vol. 3, pp. 501-508, 2006.

[46] Y. Yusoff, R. Ismail, and Z. Hassan. "Common Phases of Computer Forensic Investigation Models" International Journal of Computer Science and Information Technology, vol. 3. pp. 17-31, June, 2011.

[47] C. Soutar, and D. Roberge."Biometric Encryption" Department of Electrical and Computer *Engineering, Carnegie Mellon University Journal*, vol. 5, 2008.

[48] B. David, and G.O. Dmitry. "Assessment of Privacy Enhancing Technologies for Biometrics", in *Proceedings of IEEE International Conference on Biometrics Technology*, pp. 105-116, 2011.

[49] S. C. Ricci Ieong. "Digital Forensic Investigation Framework that Incorporates Legal Issues" *Elsevier publication*, pp. 29-36, 2006.

[50] R. S. George, and Weir Michael Daley. Issues in Cyber forensics Perspectives", in *Proceedings of the International Conference on Cybercrime, Security and Digital Forensics,* 2013, pp.120-128.

[51] A. Fragkiadakis, E. Tragos, and I. Askoxylakis. "A survey on Security Threats and Detection Techniques in Cognitive Radio Network. *IEEE Publications*." 2012, pp. 1-8.

[52] A.Al-Net, R.S George Weir, "Special Issue on Cybercrime Prevention, Detection and Response". *International Journal of Electronic Security and Digital Forensic,* vol. 5, No. 2, pp 523-530, 2013.

[53] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. *Handbook of Fingerprint Recognition*. Springer-Verlag, 2009.

[54] S. Al-Fedaghi, B. Al-Babtain and M. Al-Fahad, "Purpose-based Versus Flow-based Access Control for Privacy," *International Journal of Computer Science*, vol. 8, issue 4, pp. 564572, 2012.

[55] L. Ovie, K. C. Stephen, and B. T. Song. "Computer Forensics: Digital Forensic Analysis Methodology" *International Journal of Computer Forensics*, Volume 56, Number 1, January 2008.

[56] S. Al-Fedaghi S, and B. Al-Babtain. "Modeling the Forensics Process" *International Journal of Security and Its Applications*, vol. 6, No. 4, pp. 97 – 108, October, 2012.

[57] M. Pollitt. "A History of Digital Forensics" *International Journal of Advances in Information and Communication Technology*, vol. 337, pp. 3-15, 2010.

[58] The history of Computing Project, "Timeline: Chronology of the history of computing" *in proceedings of the history of Computing Foundation*, Maurik, 2010.

[59] D. Parker. Crime by Computer, Scribner"s, New York, 1976, pp. 1-320.

[60] C. Stoll. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage*. Pocket Books, New York, 1990, pp. 16-17.

[61] C. Whitcomb. "A historical perspective of digital evidence, *International Journal of Digital Evidence*" vol. 1, issue 1, pp. 96-102, 2002.

[62] K. Hafner and J. Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Touchstone, New York, pp. 1-136, 1991.

[63] B. J. Rothstein, R.J. Hedges, E.C. Wiggins, F.J. Center. *Managing discovery of electronic information: A pocket guide for judges.* Washington, D.C. CQ Press, 2011, 225-250.

[64] G. S. Burdynski Jr. "The Charley Project" Internet: www.charley project.org/cases/b/burdynski george.html.

[65] R. Downing. "G-8 initiatives in high tech crime" *in proceedings of the Asia-Pacific Conference on Cybercrime and Information Security*, 2002, pp. 91-106.

[66] M. Pollit, "G8 Principles for the Procedures Relating to Digital Evidence," *International Organization on Computer Evidence*, pp. 220- 225, Ottawa, Canada, 2000.

[67] M. Noblett, The development of forensic tools and examinations for data recovery from computer evidence" *in proceedings of the Eleventh INTERPOL Forensic Science Symposium*, pp. 520- 526, 1995.

[68] M. K. Rogers, K. Seigfried. "The future of computer forensics: a needs analysis survey" Center for Education and Research in Information Assurance and Security, *Purdue University Publication,* 656 Oval, West Lafayette, IN 47907, USA, 6 January, vol. 23, issue, pp. 12-16, 2004.

[69] J. Neuner, Pamela Bordner. "American Society of Crime Laboratory Directors – Laboratory Accreditation Board," Garner, North Carolina. Internet: www.ascld-lab.org. June, 03, 2015.

[70] North Texas Regional Computer Forensics Laboratory, Dallas, Texas. Internet: www.ntrcfl.org/index.cfm.

[71] U.S. General Accounting Office, Crime Technology: Department of Defense Assistance to State and Local Law Enforcement Agencies, Letter Report GAO/GGD-00-14, Washington, DC. Internet: http://opendl.ifip-tc6.org/db/conf/ifip11-9/df2010/Pollitt10.pdf, 1999 [June, 2015]

[72] RCFL National Program Office, Regional Computer Forensics Laboratory, Quantico, Virginia. Internet: www.rcfl.gov. June, 2015.

[73] Federal Judicial Center, Materials on Electronic Discovery: Civil Litigation, Federal Judicial Center Foundation, Washington, DC. Internet: www.fjc.gov/public/home.nsf/pages/196. June, 2015.

[74] M. Mason, "Congressional Testimony, Statement before the house Judiciary Committee, Federal Bureau of Investigation, Washington DC. Internet: www.fbi.gov/congress/congress07/mason101707.htm, 2007 [June, 2015].

[75] ASTM International, ASTM E2678-09 Standard Guide for Education and Training in Computer Forensics, West Conshohocken, Pennsylvania. Internet: www.astm.org/Standards/E2678.htm, 2009 [June 2015].

[76] M. T. Britz. "Computer Forensics and Cyber Crime: An Introduction" (2nd edition). Prentice Hall, New Jersey, 2004, pp.230-240.

[77] Duane B, Sankar B. "Biometric History", *Publication of the National Science and Technology Council*, pp. 1-27, August, 2007.

[78] N. S. Sargur, C. Huang, S. Harish, V. Shah. "Biometric and Forensic Aspects of Digital Document Processing," in proceedings of the International conference on Biometrics, 2010, pp. 720-728.

[79] K. Anil. I.Jain, A. Kumar. "Biometrics of Next Generation: An Overview" *Springer Publications,* pp. 27-38, 2010

[80] DNA Fingerprint Identification. http://www.fingerprinting.com/dna_fingerprint_identification.php, 20 February 2010 [June, 2015].

[81] R. Zhou, D. Zhong, and J. Han, "Fingerprint Identification Using SIFT-Based Minutia Descriptors and Improved All Descriptor-Pair Matching," *Sensors Publications*, vol. 13, pp. 3142-3156, 2013.

[82] V. Androunikou, D. Demetis, and T. Varvarigou, "Biometric implementations and the implications for security and privacy," *Journal of the Future of Identity in the Information Society*, vol. 1, pp. 20-35, 2005.

[83] A. Moenssens, *Fingerprint Technologies* "Chilton Book Company, London, 1971, pp. 123-352.

[84] A. K Jain, R. Bolle and S. Pankanti. *Biometrics. Personal Identification in Networked Society*. 233 Spring Street, New York, USA. 1999, pp. 1-220.

[85] H. C. Lee, and R.E. Gaesnselen. *Advances in Fingerprint Technology. Elsevier Publishers*, New York, 1999, pp.220-330.

[86] H. Cummins, and C. Mildo. *Fingerprints, Palms and Soles*. Dover Publication Inc. New York, 1961, pp. 20-35.

[87] K. Anil, and A,Ross."Biometrics: A Tool for Information Security" *IEEE Transactions on Information Forensic, and Security*, vol. 1, June 2006.

[88] E. Mewham. The Biometric Report, *SJB Services*, New York, 1995.

[89] Federal Bereau of Investigation. *The Science of fingerprint: Classification and Uses*. U.S, Government printing office, Washinton, D.C, 1984.

[90] A. K. Jain A; A. Ross, and S. Pankanti; "Biometrics: A Tool for Information Security; *IEE Transactions on Information Security*", vol. 2, pp. 125-143, 2006.

[91] J. Schneider and D. Wobschall. "Live Scan Fingerprint Imagery using high Resolution CScan Ultrasonography," *in proceedings of the 25th International Conference on Security Technologies*, 1996, pp. 88-95.

[92] R. J. Vacca. "*Handbook of Sensor Networking*," R. J. Vacca. Taylor and Francis Group, 2015.

[93] K. McCalley, D. Setlak, S. Wilson, and J. Schmitt. "A direct fingerprint reader", *in proceedings of the CardTec/Secure Conference*, vol 1, 1993, pp. 271-279.

[94] F. R. Livingstone, L. King, J. Beraldin, and M. Rioux. "Developement of a Real Time Scanning System for Object Recognition, Inspection, and Robot Control," *in proceedings of SPIE on Telecommunication Technology and Space Telerobotics,*" vol. 2057, Sep.1993, pp. 451461.

[95] M. Hartman. "Compact Fingerprint Scanner Techniques," *in proceedings of the 8th Meeting of the Biometric Consortium*, San Jose, California, June, 1996, pp. 520-527.

[96] E. Botha, and L.Coetzee. "Fingerprint Recognition with a Neural-net Classifier," *in proceedings of the 1st South Africa Workshop on Pattern Recognition,*" vol.1, 1990, pp. 33-40.

[97] L. E Sánchez, A. S.O. Parra, "Managing Security and its Maturity in Small and Mediumsized Enterprises, "*Journal of Universal Computer Science*, vol. 15 (15), 3038 – 3058, 2009.

[98] A. L. Opdahl, and G. Sindre, "Experimental Comparison of Attack Trees and Misuse Cases for Security Threat Identification," *Information and Software Technology*. In Press, Corrected Proof, 2008.

[99] P. Hunton. "The Stages of Cybercrime Investigations: Bridging the Gap between Technology Examination and Law Enforcement Investigation," *Computer Law and Security Review*, pp. 61-67, 2011.

[100] H. Mouratidis, C. Kalloniatis, S. Islam, H. Mrc-Philippe, S. Gritzalis. "Aligning Security and Privacy to Support the Development of Secure Information Systems", *Journal of Universal Computer Science*, vol. 18, no. 12, pp. 1608-1627, 2012

[101] R. Rastogi, S. Ruw von. "Information Security Service Culture – Information Security for End-users", *Journal of Universal Computer Science*, vol. 18, no. 12, 1628-1642, December, 2012.

[102] P. Martinez-Julia, A. F. Gomez-Skarmeta. "A Novel Identity-based Network Architecture for Next Generation Internet", *Journal of Universal Computer Science*, vol. 18, no. 12, pp. 16431661, June, 2012.

[103] T. Baars, "M. Spruit. "Analysing the Security Risks of Cloud Adoption Using the SeCA Model: A Case Study", *Journal of Universal Computer Science*, vol. 18, no. 12, pp. 1662-July, 2012.

[104] S. Ngobeni, H. Venter, "The Modeling of a Digital Forensic Readiness Approach for Wireless Local Area Networks," *Journal of Universal Computer Science*, vol. 18, no. 12, 17211740, June, 2012.

[105] D. Mellado. "An Overview of Current Information Systems Security Challenges and Innovations," *International Journal of Universal Computer Science*, vol. 18, pp.159-1608, 2012.

[106] M. F. Islam, M. I. Nasrul. "A Biometrics-Based Secure Architecture for Mobile Computing," *IEEE Transaction on Biometric Authentication*, vol. 8, pp. 520-528, 2009.

[107] H. Singh Lallie. "An Overview of the Digital Forensic Investigation Infrastructure of India, Digital Investigation - *Online publication*. pp. 1742-2876, March, 2012.

[108] L. Simson, Garfinkel. "Digital forensics research: The next 10 years," *Elsevier Journal on digital investigation,* vol.7, pg. 64-73, 2010.

[109] V. Baryamureeba, and F. Tushabe. "The Enhanced Digital Investigation Process Model, *in proceedings of the Fourth Digital Forensic Research Workshop*, May 27, 2004, pp. 115-122.

[110] Aleksandar Valjarevic, HS Venter. "Towards a Digital Forensic Readiness Framework for Public Key Infrastructure Systems," *IEEE Publications*, vol. 10, issue 5, pp. 115-122, 2011.

[111] Y. Yusoff, R. Ismail, and J. Hassan. "Common Phases of Computer Forensic Investigation Models" *International Journal of Computer Science and Information Technology*," vol. 3, issue 3, pp. 17-31, 2011.

[112] R. Lee. "Forensic and Investigative Essentials," *in proceedings of Sans Institute Forensics 508: Advanced Computer Forensic Analysis and Incident Response Training*, Washington, DC, 2010, pp. 1-35.

[113] I.O. Ademu , and C.O. Imafidon, "Applying Security Mechanism to Digital Forensic Investigation Process". *International Journal of Emerging trends in Engineering and Development,* vol. 7, issue 2, pp.128-132, 2012.

[114] L. Leutele, M. Grey, and C. Steve. "Computer (Digital) Forensic Tools and Biometric," *Academic International Journal*, pp. 1-15, November 2013.

[115] L. C. Ovie, K. B. Stephen, and S. Thomas. "Computer Forensics: Digital Forensic Analysis Methodology," *Computer Forensics Journal,* vol. 56, No 1, pp. January 2008.

[116] M. Meyers, M. Rogers. "Computer Forensics: The need for Standardization and Certification."Internet:http://www2.tech.purdue.edu/cpt/courses/CPT499S/meyersrogers_ijde.pdf, October, 2004

[117] K. M. Enos, H. S Venter. "State of the art of Digital Forensic Techniques," *in proceedings of the ISSA Conference*, 2011, pp. 1-7.

[118] P. D Dixon. "An overview of computer forensics". *IEEE Potentials*, vol.24, issue 5, pp. 117-127, 2005.

[119] D. Ayers. "A second generation computer forensic analysis system," *in proceedings of the 9th Annual DFRWS Conference*, vol. 6 (Supplement 1), pp. 34-42, 2009.

[120] C. W. Adams,. "Legal issues pertaining to the development of digital forensic tools," *in proceedings of the - SADFE 2008 3rd International Workshop on Systematic Approaches to Digital Forensic Engineering*, Berkeley, May, 2008, pp.123 – 132.

[121] B. Schneier. *A Self-Study Course in Block-Cipher Cryptanalysis, Cryptologia.* [online], Taylor and Francis, vol. 2, issue 1, pp. 18–34, January 2000.

[122] P.A. Wertheim. "Scientific Comparison and Identification of Fingerprint Evidence", vol. 26 No. 101, 2000, pp. 95-106.

[123] D. J. Thornton. "Setting Standards in the Comparison and Identification," *in proceedings of the 84th Annual California State Division of IAI Laughlin Training Conference*, Nevada, 2000.

[124] D.S, Jadhav, A.P, Ghatulu. "A Study of the Analysis Techniques to gather Evidence for Presentation in the Legal Constitution," *International Journal of Research in Information Technology and Sciences*, vol. 2, pp. 235-243, 2012.

[125] Scientific Working Group on Friction Ridge Analysis, Study and Technology (SWGFAST). Internet: http://www.swgfast.org/, May 2015.

[126] "A Simplified Guide To Fingerprint Analysis" *National Forensic Science Technology Center NFSTC Science Serving Justice, Publication,* 7881 114th Avenue North Largo, Florida, 33773 (727), pp. 549--6067. Internet: info@nfstc.org

[127] Saferstein, Richard. *Criminalistics: An Introduction to Forensic Science.* Pearson Education, Inc., Upper Saddle River, NJ. pp. 502-5020. 2007.

[128] D. McClure. Group on "Scientific and Forensic Evidence in the Courtroom." Internet: https://www.ncjrs.gov/pdffiles1/nij/grants/220692.pdf, March 2007, [May 2015].

[129] D.P Lyle. *Forensic for dummies*. Wiley Publishing, Inc., 111 River St. Hobooken, NJ, 07030-5774, 2004, pp. 1-24.

[130] Paul C. Giannelli. "The Admissibility of Novel Scientific Evidence," *Columbia Law Review Association, Inc.*, vol. 80, No. 6 , pp. 1197-1250, Oct., 1980.

[131] D. Chris Lennard "The Detection and Enhancement of Latent Fingerprints" *in proceedings of the 13th INTERPOL Forensic Science Symposium*, Lyon, France, vol. 3, pp. 77- 82, Oct.2001

[132] H.H. Eric, L. O. Robinson, J. H. Laub. *The Fingerprint Source Book.* National Intitute of Justice, U.S. Department of Justice,Office of Justice Programs, 810 Seventh Street N.W, Washington, DC 20531, 2010, pp.6-29.

[133] Trier O.D, "Goal-directed evaluation of binarization methods" *IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI),* vol. 17, Issue 12, pp.1191-1201, 2002.

[134] Y. Li, and X. Xu, "Revolutionary Information System Application in Biometrics," *in proceedings of the International Conference on Networking and Digital Society, ICNDS'09*, 2009, pp. 297-300.

[135] L. Frye, F. Gamble, and D. Grieser. "Real-time fingerprint verification system," *OSA Publications,* vol. 31, issue 5, pp. 652-655, 1992.

[136] N, Ratha, R. Bolle. *Automatic comparison of fingerprint-ridge patterns.* Springer Verlag, New York, Inc. 2004, pp. 1-125.

[137] M. El-Abed, C. LaCharme, and, C. Rosenberger. "Privacy and Security Assessments of Biometrics Systems," Biometric Security, *Cambridge Scholars Publishing*, New Castle upon Tyne, UK, 2015, pp. 224-254.

[138] U. Uludag, and A. K. Jain. "Attacks on biometric systems: a case study in fingerprints," *in proceedings of the SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, CA, vol. 5306, 2004, pp. 622-633.

[139] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz. "Evaluation of direct attacks to fingerprint verification systems," *Journal of Telecommunication Systems*, vol. 47, issue 3-4, pp. 243-254, 2011.

[140] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. "An evaluation of indirect attacks and countermeasures in fingerprint verification systems," Pattern Recognition Letters, *Elsevier Publications*, vol. 32, pp. 1643-1651, 2011.