2020-03

Development of secured algorithm to enhance the privacy and security template of biometric technology

Habibu, Taban

NM-AIST

http://doi.org/10.58694/20.500.12479/900

DEVELOPMENT OF SECURED ALGORITHM TO ENHANCE THE PRIVACY AND SECURITY TEMPLATE OF BIOMETRIC TECHNOLOGY

Taban Habibu

A Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Mathematical and Computer Science and Engineering of the Nelson Mandela African Institution of Science and Technology

Arusha, Tanzania

March, 2020

ABSTRACT

The security of information and personal privacy are the growing concerns in today's human life worldwide. The storage of biometric data in the database has raised the prospect of compromising the database leading to grave risks and misuse of the person's privacy such as growth in terrorism and identity fraud. When a person's biometric data stored is revealed, their security and privacy are being compromised. This research described a detailed evaluation on several outbreaks and threats associated with the biometric technology. It analyzed the user's fear and intimidations to the biometric technology alongside the protection steps for securing the biometric data template in the database. It is known that, when somebody's biometric data template is compromised from the database that consequently might indicate proof of identity robbery of that person. Mixed method to compute and articulate the results as well as a new tactic of encryption-decryption algorithm with a design pattern of Model View Template (MVT) are used for securing the biometric data template in the database. The model managed information logically, the view indicated the visualization of the data, and the template directed the data migration into pattern object. Factors influencing fear of biometric technology such as an exposer of personal information, improper data transfer, and data misuse are found. Strong knowledge of the ideal technology like the private skills of the biometric technology, data secrecy and perceived helpfulness are established. The fears and attacks along the technology like a counterfeit of documents and brute-force attack are known. The designed algorithm based on the cryptographic module of the Fernet keys instance are utilized. The Fernet keys are combined to generate a multiFernet key, integrated with biometric data to produce two encrypted files (byte and text file). These files are incorporated with Twilio message and firmly stored in the database. The storage database has security measures that guard against an impostor's attack. The database system can block the attacker from unauthorized access. Thus, significantly increased individual data privacy and integrity.

DECLARATION

I, Taban Habibu, do hereby declare to the Senate of the Nelson Mandela African Institution of Science and Technology that this Thesis is my own original work and that it has neither been submitted nor being concurrently submitted for degree award in any other institution.

1st / April / 2020

Taban Habibu
Name and Signature of Candidate

Date

The above declaration is confirmed

1st April, 2020

Dr. Anael Elikana Sam
Name and Signature of Supervisor 1

Date

1st April, 2020

Dr. Edith Talina Luhanga
Name and Signature of Supervisor 2

Date

COPYRIGHT

CERTIFICATION

The undersigned certify that they have read and hereby recommend for examination a Thesis entitled *Development of Secured Algorithm to Enhance the Privacy and Security Template of Biometric Technology*, in fulfilment of the requirements for the degree of Doctor of Philosophy of the Nelson Mandela African Institution of Science and Technology.

Dr. Anael Elikana Sam

(Supervisor)

Date: 1st April, 2020

Dr. Edith Talina Luhanga

(Supervisor)

Date: 1st April, 2020

ACKNOWLEDGMENT

First and foremost, I thank the Almighty Allah for the gift of life, wisdom, strength and good health, as considerably as for His guidance, protection and love to enable me to complete the PhD program successfully, without whom none of my effort would have counted.

I extend my special thanks to my supervisors Dr. Anael Elikana Sam and Dr. Edith Talina Luhanga of Nelson Mandela African Institution of Science and Technology (NM-AIST), Arusha, Tanzania, for their invaluable guidance and support throughout my research. They ensured that I made adequate progress in my research and offered useful corrective suggestions throughout. I remain thankful for their vast knowledge and sagacity which has made my PhD research a tremendous learning experience.

My thanks are also due, albeit posthumously, to the late Dr. Yaw Nkansah-Gyekye who was my first supervisor, a mentor and inspiration to me for the sounder part of one year of my three-year stay at NM-AIST. I will not forget his constant encouragement to complete my studies on time. My deep gratitude and appreciation to the NM-AIST Community, School of Computational and Communication Sciences and Engineering (CoCSE), the NM-AIST CoCSE lab technicians, Librarians and the staffs of NM-AIST, Late Prof. Alfred N. Muzuka, Prof. Dmitry Kuznetsov, Prof. Verdiana Masanja, Dr. Shubi Kaijage, Dr. Kisangiri Michael, Dr. Dina Machuve, Dr. Mussa Ally, for their extensive feedback and valuable suggestions regarding the study.

I extend my sincere, deepest gratitude to my brothers and sisters, you are always there for me and I can’t measure your supports, care, love, advice, encouragement and understanding, Ustadh Badru Khamis, Ali Hamid, Ramadhan Khamis, Ratibu Khamis, Ismail, Mustafa, Salama and Zura. May almighty Allah rewards you all abundantly. I do not forget to thank my colleagues and my extended network of friends, Guma Ali, Cleverence Kombe, Marseline Michael Mtey, Mathias Ombeni, Neema Mduma, Juliana S. Kamaghe, Sarah Nyanjara, Judith Leo, Devotha Nyambo, Juliana Mandha, Kafula Chisanga, Difo Voukang Harouna, Mikaila Garko, Elmugheira Mockarram, Ssemwanga Mohammed, etc., for the mutual encouragement we shared, May God bless you all.

I owe so much to my family for the moral and emotional support they continue to provide. They deserve very special mention as they had to put up with my absence for much of the past three years. Your advices, prayers and moral support were always igniting up in me a fresh spirit to press on. My wife Naima Habibah and children's, Hamidah, Hajiba, Rayat, and Abdul Rauf. When I was home and busy working on my research, they were very understanding and gave me the time and space I needed to complete my research. May almighty Allah rewards you all profusely.

All this work could not be possible without the financial support under the Higher Education, Science and Technology (HEST) Project Staff Capacity Development Fund. This scholarship could not have come at a better time than it did, and I will never cease to be appreciated for it. I wish to thank my employers at the Muni University (MU) for granting me study leave to enable me to pursue my studies in Tanzania. In particular, Prof. Christine Dranzoa, Prof. Simon Anguma Katrini, Rev. Fr. Dr. Odubuker Picho Epiphany, Dr. Alumai Alfred, Dr. Andogah Geoffrey and Mr. Abdul Wahid Ijosiga. They deserved special mention as the one who believed in me and played a significant role in securing funding for my studies under African Development Bank (AfDB) HEST Project.

DEDICATION

To my family:

Late Khamis Abdullah and Hajiba Muhammad, Ustadh Badru Khamis, Hamidah, Hajiba, Rayat, Abdul Rauf and Neima Habibah

For instilling in me the values of education and always encouraging my pursuit of knowledge, no matter where it leads me.

May Almighty Allah rewards you all profusely.

TABLE OF CONTENTS

ABSTRACT i

DECLARATION ii

COPYRIGHT iii

CERTIFICATION iv

ACKNOWLEDGMENT v

DEDICATION vii

TABLE OF CONTENTS viii

LIST OF TABLES xii

LIST OF FIGURES xiii

LIST OF APPENDICES xv

LIST OF ABBREVIATIONS AND SYMBOLS xvi

CHAPTER ONE 1

INTRODUCTION 1

1.1 Background of the problem 1

1.2 Statement of the problem 3

1.3 Rationale of the study 4

1.4 Objectives of the study 4

1.4.1 General objective 4

1.4.2 Specific objectives 5

1.5 Research questions 5

1.6 Significance of the study 5

1.7 Delineation of the study 6

CHAPTER TWO 7

LITERATURE REVIEW 7

2.1 Introduction 7

2.2 Biometric operational mechanisms 7
2.3 Biometric system performance 9
2.3.1 The matching error 9
2.3.2 The acquisition error 10
2.4 The vulnerability and attacks against biometric technology 12
2.4.1 Direct and indirect attack 13
2.4.2 Repudiation 14
2.4.3 Coercion 14
2.4.4 Administrative fraud 14
2.4.5 Sensor attacks 14
2.4.6 Character extractor attacks 15
2.4.7 Attack on database template 15
2.5 Privacy and security risks of the biometric technology 18
2.5.1 Privacy issue 18
2.5.2 Security issue 19
2.5.3 Weakness of the biometric technology 19
2.6 Biometric template protection measures 20
2.6.1 Hardware-based level 21
2.6.2 Software-based level 21
2.6.3 The feature transformation 22
2.6.4 Biometric cryptosystem 24
2.7 Techniques to secure data storage 25
CHAPTER THREE 29
MATERIALS AND METHODS 29
3.1 Introduction 29
3.2 Study design 29

3.3 Population and sampling procedure 29
3.4 Data collection 29
3.5 The case studies and documentation 30
3.6 Data analysis 30
3.7 Validity and reliability 31
3.8 Ethical consideration 31
CHAPTER FOUR 32
RESULTS AND DISCUSSION 32
4.1 Introduction 32
4.2 Social demography characteristic 32
4.3 Factors determining the acceptance of the biometric application 33
4.4 The biometric data secrecy 35
4.5 Factors that influence individuals' distress of the biometric application 37
4.6 The security threats of the biometric technology 38
4.7 Protective measures of the biometric data 42
4.8 The existing biometric passport system 43
4.9 The proposed system of the biometric application 44
4.10 Security tools used to protect the biometric data template 46
4.10.1 Jinja2 47
4.10.2 Wtforms 47
4.10.3 SQLAlchemy 48
4.10.4 The cryptography 49
4.10.5 The Twilio SMS programmable 49
4.10.6 The suggested MVT-HUF architecture 50
4.11 The proposed encryption-decryption algorithm and database model 51
4.11.1 The encryption algorithm 51

4.11.2 The decryption algorithm 53
4.11.3 Database models 55
4.12 The implementation and evaluation process 55
4.12.1 The cryptographic of Fernet keys 56
4.12.2 The key management for the encryption algorithm 57
4.12.3 The multiFernet encryption algorithm 58
4.12.4 The key management for the decryption algorithm 58
4.12.5 The performance evaluation of the algorithm 59
4.13 Discussion of the results 60
4.13.1 How secure is biometric technology used in the biometric passport acquisition? 61
4.13.2 How people's biometric data are being handled during the passport issuance? .. 61
4.13.3 What is the potential privacy-security risks and users' fears regarding the biometric technologies? 62
4.13.4 What countermeasure do users recommend to protect the biometric data template in the database? 62
CHAPTER FIVE 65
CONCLUSION AND RECOMMENDATIONS 65
5.1 Conclusion 65
5.2 Recommendations 66
REFERENCES 68
APPENDICES 84
RESEARCH OUTPUTS ..... **Error! Bookmark not defined.**

LIST OF TABLES

Table 1: Comparison of biometric characteristics (H=high, M=medium, L=low).....12

Table 2: The possible attacks with reference to Fig. 3 attack point.....17

Table 3: The biometric data secrecy 37

Table 4: The biometric characteristics.....42

LIST OF FIGURES

Figure 1: Enrollment and verification of the biometric authentication process.....8

Figure 2: (a) False match rate and false non-match rate for a given threshold t (b) The curve linking FMR to FNMR.....11

Figure 3: The vulnerabilities and attacks of the biometric technology.....13

Figure 4: Categorization of the biometric template protection scheme.....21

Figure 5: Basic concept of biometric key binding.....24

Figure 6: The social demography features of the participants (a) Gender, (b) Professionalism, (c) Experience on biometric features, (d) Security of biometric.....33

Figure 7: Utilization of the biometric passport technology.....35

Figure 8: Factors influencing users fear of the biometric application.....38

Figure 9: (a) The threats of the biometric technology (b) The attack of the biometric technology.....40

Figure 10: The biometric modalities.....41

Figure 11: (a) The protection mechanism of the biometric technology, (b) The privacy enhancement of the biometric technology.....43

Figure 12: The existing framework of the biometric passport system.....44

Figure 13: (a) Twilio verification message (b) Twilio message for the biometric scan.....45

Figure 14: The proposed architecture of the biometric application system.....46

Figure 15: The SQLAlchemy dependencies layers.....48

Figure 16: (a) The framework model of the MVT-HUF system, (b) The function design of the ePassport.....51

Figure 17: The proposed framework of the encryption algorithm.....52

Figure 18: The proposed framework of the decryption algorithm.....53

Figure 19: The proposed framework for the security mechanism.....54

Figure 20: The SQLite3 database classes 55

Figure 21: The AES Block 56

Figure 22: The key management of the encryption algorithm 57

Figure 23: The multiFernet key implementation 58

Figure 24: The key management of the decryption algorithm 59

Figure 25: The client-server architecture 63

LIST OF APPENDICES

Appendix 1: Qualitative questionnaires for passport issuance officers 84

Appendix 2: Quantitative questionnaires for document owners 91

Appendix 3: Introduction letter from the school of CoCSE 97

Appendix 4: Introduction letter from the office of Deputy Vice Chancellor 98

Appendix 5: Python code for account creation, Login and template rendering 99

Appendix 6: Python code for biometric feature Scanning 101

Appendix 7: Python code for facial extraction and encryption-decryption process 104

Appendix 8: Python code for Cryptography key generation 108

Appendix 9: Python code for encryption algorithm process 109

Appendix 10: Python code for decryption algorithm process 110

Appendix 11: Python code for Database model settings.....111

Appendix 12: Python code for biometric template and biodata encryption 112

Appendix 13: Python code for Twilio SMS 114

LIST OF ABBREVIATIONS AND SYMBOLS

AC	Authentication Code
AES	Advance Encryption Standard
AfDB	African Development Bank
API	Application Program Interface
ATM	Automated Teller Machines
CBC	Cipher Block Chaining
CCC	Chaos Computer Club
CCTV	Closed Circuit Television
CoCSE	Computational and Communication Sciences and Engineering
CRM	Customer Relationship Management
CSRF	Cross Site Reference Forgery
Dell	Digital Electronic Link Library
DoS	Denial-of-Service
DoS	Denial-of-Service
EAC	East African Community
EER	Equal Error Rate
EER	Equal Error Rate
FAR	False Acceptance Rate
FC	Fuzzy Commitment
FE	Fuzzy Extractor
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
FTC	Failure to Capture

FTE	Failure to Enroll
FV	Fuzzy Vault
GAR	Genuine Accept Rate
HEST	Higher Education Science and Technology
HMAC	Hash-Based Message Authentication Code
Hp	Hewlett Packard
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HUF	Helper Utilities Filesystem
ICT	Information and Communication Technology
ID	Identifications
IEC	International Electrotechnical Commission
IoT	Internet of things
ISO	International Organization for Standard
IT	Information Technology
IUID	Indian Unique identification
IV	Initialization Vector
MCC	Minutia Cylinder Code
MRZ	Machine Readable Zone
MU	Muni University
MVC	Model View Controller
MVT	Model View Template
NGI	Next Generation Identification
NIC	National Identity Card
NIRA	National Identification and Registration Authority

NIST	National Institute of Standards and Technology
NM-AIST	Nelson Mandela African Institution of Science and Technology
ORM	Object Relational Mapper
PCB	Printed Circuit Board
PII	Personal Identifiable Information
PIN	Personal Identification Number
RFID	Radio Frequency Identification
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SMS	Short Message Service
SPSS	Statistical Package for Social Sciences
SQL	Structured Query Language
TCG	Trusted Computing Group
TPM	Trusted Platform Module
USA	United States of America
USB	Universal Serial Bus
XSS	Cross Site Scripting

CHAPTER ONE

INTRODUCTION

1.1 Background of the problem

The biometric is derived from the Greek words bios “life” and metrics “measure” (Ambalakat, 2005; Ashok & Shivashankar, 2006). Its pattern is to identify, recognize and verify users based on their unique traits such as physiological characteristics (Fingerprint, Palm Print, Face and Iris) and behavioral characteristics (Signature, Keystroke and Giant). The voice can either be physical or behavior traits. Today’s human verification factors are categorized into three; Things you know, e.g. secret password, Personal Identification Number (PIN); Things you hold, smart card etc., and who you are, biometrics (Jain, Flynn & Ross, 2007). However, the first two factors can be tricked. For example, password and PINs can be given to different person, perhaps causing an identity robbery or misuse (Jain *et al.*, 2007). Besides, it can be illegally taken from straight look. Once an intruder has the password, the person has total access to the related resource. The foremost benefit of biometrics is persons identification, it entails the individual presences at the stage of the validation convenience (Prabhakar, Pankanti & Jain, 2003).

Currently the biometric technologies are used in laptops and smartphones. Many of the largest Internet of things (IoT) players, Microsoft, Google, Samsung, Tecno and Apple are already offering biometric verification as an entity in some products and are working on deploying more and extend further into the households and businesses. Digital electronic link library (Dell), Hewlett Packard (Hp) among other technologies comes with inbuilt digital web camera that can scan individual characters for verification, such as simplest attendance or time applications to most sophisticated security access control installation. The high-scale initiatives, like the Indian Unique Identification (IUID) of the India government (Jacobsen, 2012) and European Commission (Sontowski, 2018), have currently embraced biometrics as their recognition technology.

However, irrespective of the vital development in the current eras, the biometric encounters intimidations (Bolle, Connell & Ratha, 2002). The primary worry is user’s secrecy and security dangers. When a person’s biometric data is hijacked, the attacker can utilize it to pretend as the individual, or simply scan that individual’s remote activity (Pratiba & Shobha, 2013).

The world's premier technical security conference organized by the University of Hanoi (Vietnam) in 2009, demonstrated how biometric system can simply be tricked and bypassed. Fake face image of the lawful user is utilized, within a few moments, authorization access is gained into the application. The susceptibility is immediately recorded in the nationwide database, National Institute of Standards and Technology (NIST). The Apple Inc. in 2013, set a novel device, iPhone 5s with fingerprint instrument for login to secure users' data. Fewer than two days subsequently, German hacker using gummy fingerprint successfully confirmed the spoofed device. These confirmed quite a few others, the intimidations and exposures in the present biometric based data protection.

In Uganda, the problems associated with biometrics technology are exposer of personal data, data misuse (maltreatment) and improper data transfer as well as threats and attacks such as, counterfeit of documents and brute-force attack. For instance, fifteen-thousand-two-hundred and seventy-seven million thumbprints intended for National Identity Cards (NIC) is pulled out from National Identification and Registration Authority (NIRA) database storage, elevated serious worry to citizens (Rindai, 2016). Although some observers appreciated it as a full exercise against scam deterrence and individuality, the fear for citizens' secrecy and security of the biometric data template in the database remained a big research query. It can also be realized that, in 2001, the state of Colorado tried to sell their face and fingerprint database to any government agency that wants access (Krause, 2001). This jeopardizes individual safety and identity.

According to Kumar and Srinivasan (2013) if a person request, for instance, a permit, the government holds the evidence. The data submitted cannot be deleted, it's compromised forever, only with a smart card, the bank can create the individual a new card with different PIN, because a user has merely a restricted number of biometrics, one face, 10 fingers, and two irises which are hardly replaceable.

Consequently, protecting and securing the biometric data template in the database server against the secrecy and security infringement is really paramount, because it helps provide popularize usage of biometric with increasing user adoption and ensure trust in the scheme and with people working in the application. Therefore, countermeasure to a spoofing attack is required like liveness detection to spot some biological signs as well as an encryption-decryption algorithm in securing the biometric data in the storage (Kalvet, Karlzén, Hunstad

& Tiits, 2018). It assumed that multi-modal systems (e.g. combining face, fingerprint or iris biometric modalities) is harder to spoof than unimodal systems.

1.2 Statement of the problem

With the prevalent deployment of biometric technology, such as travel document, national identification, mobile transaction system, among others, users' concerns about privacy and security risks of biometric data template in the database remain a big study issue *(*Avoine, Kalach & Quisquater, 2008; Jeng & Chen, 2009). Because the storage data template in the database can be replaced with impersonator's trait. The impostor can generate spoofing from the unique trait to obtain illegitimate entry to genuine individual's data, i.e., Health history. The impostor can use the stolen genuine template of an individual to counterfeit documents and in return, results into Denial-of-service (DoS) for that particular individual (Ghouzali *et al.*, 2016; Riaz, Alfred & Khan, 2018). The fact that, the biometrics data template cannot be altered or replaced like passwords and PINs, creates a chance for an impostor to modify and substitute the genuine biometric data template with the fake one (Arjunwadkar, Kulkarni & Shahu, 2012).

Several approaches for securing template database have been suggested. Yang, Wang, Hu, Zheng and Valli (2019) surveyed the security and accuracy of fingerprint-based biometric template to identify vulnerability attacks to template database. Rosenberger (2018) discussed the valuation of biometric template protection mechanism based on a transformation. Maniroja and Sawarkar (2013) discussed biometric database safety using public key cryptography of biometric authentication systems. Mwema, Kimani and Kimwele (2015) analyzed the methods and measures intended for safeguarding biometric fingerprint templates.

Nevertheless, most of the study did not report the common weakness related to privacy and security risks, where biometric information in the database is retrieved without the user's awareness; unauthorized party succeeding in recovering plaintext reference of biometric data template in the database and users traceability, where an adversary can trace user's authentication attempts to access the system. This research suggested solutions based on encryption-decryption algorithm on cryptographic module, where biometric information can be encrypted using multiFernet key generated from the Fernet keys instance to guarantee that

the biometric data template stored in the database is secure and difficult for a fraud to beat or break through.

1.3 Rationale of the study

The future to sustain the identity and preserve the individual rights and freedom depends on how effectively users can deal with the information they share and the methods of attack that are being made by technological change. This study described the fear of users of biometric technology (biometric passport) and countermeasures to protect and ensure the biometric data template in the database. Use of poorly unprotected biometric template database can create loopholes for an attacker to compromise (Imamverdiyev, Teoh & Kim, 2013).

Given the above argument, lawmakers need to produce a thoroughgoing inspection to spot vital issues associated with the technology. An exhaustive investigation, especially the biometric passports, for example, can aid experts and the communities to appreciate the dangers required and take advantage of the countermeasures.

It's important for decision-makers and security experts to realize that biometric technologies often bring worries of secrecy and civil freedoms amongst the overall public. So, the user's willingness of biometric technology, reliant on the level of confidence in the technology and trust with those running the system. Therefore, the researcher sought to put up a more effective technique for securing biometric data template in the database against individual privacy and security threats. The proposed method ensured that the privacy and security risks of the biometric data as well as unauthorized access to database is secured. Because the database will block any attacker from unauthorized access and cross verify the attacker based on the validation of the ownership i.e., authentication code (AC) and sent a Twilio message to user for confirmation. In a current research study, the encryption-decryption algorithm renders more secure data protection storage (Maniroja & Sawarkar, 2013).

1.4 Objectives of the study

1.4.1 General objective

The general aim of this research is to develop a secured algorithm to enhance the privacy and security template of biometric technology, as the biometric technology applies to many different applications, the research is focused within the biometric passport. Because more

than 15.277 million Ugandan fingerprints meant for NIC were extracted from the NIRA database for voting purpose (Rindai, 2016). Yet the information is integrated with national biometric passport application.

1.4.2 Specific objectives

The specific aims of the research are:

(i) To review the current applications and vulnerabilities of biometric technology.
(ii) To analyze the enhanced factors to user's concerns and knowledge pertaining to privacy and security of biometric technology.
(iii) To design and develop an algorithm to secure the biometric data template in the database.
(iv) To validate the developed algorithm of the secured template.

1.5 Research questions

In order to carry out the research objectives, the research was guided by the following research questions:

(i) How secure is biometric technology used in the biometric passport acquisition?
(ii) How people's biometric data are being handled within the permit attainment?
(iii) What potential privacy-security dangers and users' fears are related to biometric technologies?
(iv) What countermeasure do users recommend to protect the biometric data template in the database?

1.6 Significance of the study

This work significantly contributes to the general knowledge gap intended to recognize the relevant user's fears, like an exposure of personal data, inappropriate data transfer and unauthorized access to personal data, as the anticipated concerns and perceived benefits. It provides useful and valued material for all participants (i.e., the personal identification service providers, administrations, innovators) anticipated to offer individuals this safety system in day-to-day activity. It encourages practitioners to carefully consider the potential benefits and thoroughly evaluate the risks associated with the implementation of this technology. It enables lawmakers and security experts to gain a more suitable and correct

decision for the country citizens and communities, because it's an important aspect of data security and secrecy protection. It helps build better policy on how to handle issuing of biometric passports as well as minimize the risk and circumvent, abuse of the user data (function creep). Lastly, provides useful insight and awareness to users about the safety of the data they get and supply throughout recording in everyday government or organization application activities.

1.7 Delineation of the study

The study is delimited to the followings:

(i) The research focused on users' fears of the biometric technology, taking in mind campus students, instructors and passport officer as the aspiration trial. The possibility in which penalties can be slightly changed had nationwide ID and driver's license being measured in the large study.

(ii) The access to data is very difficult to obtain from the security perspective, because sensitive private information was not revealed. There was no data record disclosed or extracted from the officers to focus on particular scenarios happening. The study only obtained data from the qualitative questionnaires designed to the key informants.

(iii) The evaluation of the algorithm was based on the inputs from the user to express their willingness to the ePassport system by considering three factors such as the performance, acceptability and the convenience. The possibility to use other testing tools could be of the great importance.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The aim of this chapter is to survey the relevant literatures on the biometric technology and the mechanism for securing the biometric data in the storage. The review is subdivided into six segments: (a) biometric operation mechanism, (b) biometric system performance, (c) vulnerability and attacks against biometric technology, (d) privacy and security risks, (e) biometric template protection measures and (f) techniques to secure the biometric data template in the database.

2.2 Biometric operational mechanisms

Biometric relies on two fundamental mechanism i.e., authentication and identification (Awad & Hassanien, 2014; Prabhakar *et al.,* 2003; Xi & Hu, 2010). The authentication is mainly to determine if a person is who she or he claims to be, for instance, an individual requires an active participation to cash a check. While identification, by contrast, capture a person's biometric data, for instance, an airport boarding gate, then compares it with the data template stored in a database looking for a match. The biometric encompasses four (4) modules: sensor module (enrollment unit), characters extraction, data record in the storage, and identical unit (Latha & Rameshkumar, 2013; Yang *et al.*, 2019). The sensor module obtains the individual's biometric sample to produce its digital representation, for instance, digital webcam for facial or scanner for fingerprint. The thumbprints (minutiae) are extracted to acquire the biometric sample via a feature extractor module (algorithm software). These features are saved as template data. The identical unit is answerable to get either like or unlike score. For instance, Alice registers her biometric data (fingerprint) with a desired server. The biometric data template is created for Alice and stored on central server or a device (Smart card) for the purpose of comparability in the confirmation phase. During the validation, Alice can provide another biometric sample, which is then compared with the data template in the server or device, if the current sample matches with the data template, she is granted access or refuse service (Xi & Hu, 2010; Yang *et al.,* 2019). Figure 1 indicated the enrollment and verification process of the biometric technology.

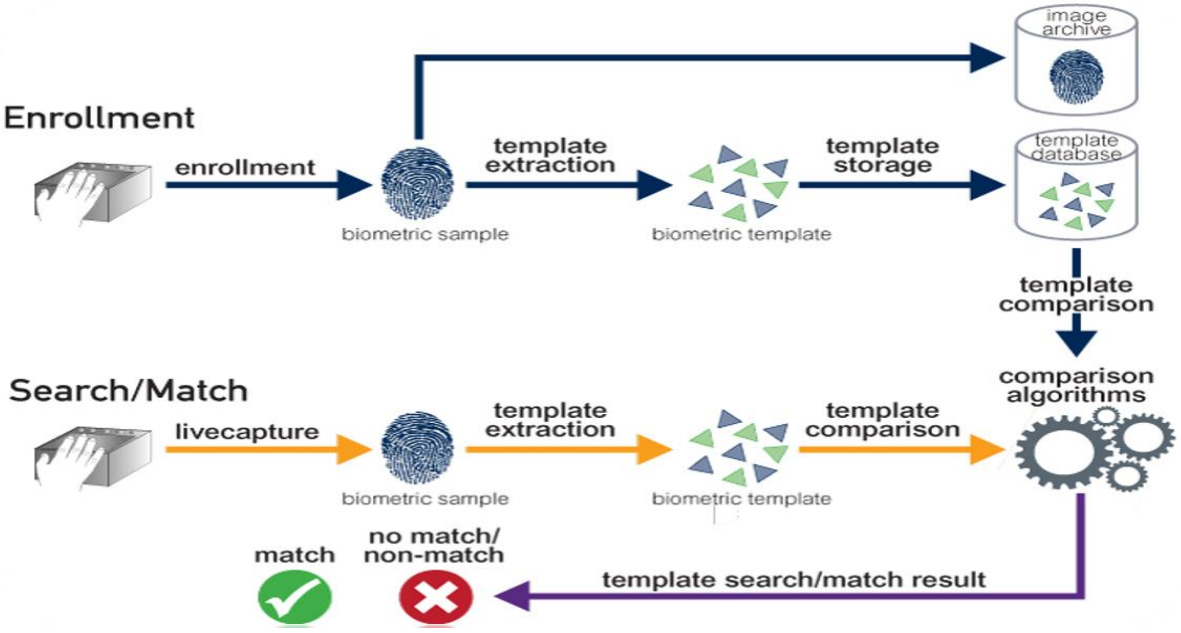


Figure 1: Enrollment and verification of the biometric authentication process (Yang *et al.*, 2019)

In Uganda, the biometric technologies are used in several private and public applications, such as law enforcement, migration border, customer or dormitory houses, and monetary facilities (Awad & Hassanien, 2014; Zheng, Fang, Shankaran & Orgun, 2015; Zheng *et al.*, 2017; Zheng, Shankaran, Orgun, Qiao & Saleem, 2017).

In the law enforcement, the biometric technology is embraced across the globe for its efficiency in security. At present, it has been launched as an international revolution in many nations, like the United States, United Kingdom, Australia and China (Yang *et al.*, 2019).

In the border control, biometric technology is used to avert counterfeit documents and strengthen the border security. Several countries employ biometric technology for securing control of travelers across borders. By 2020, 90% of the 35 million Australia, will cross via a paperless biometric recognition system. In March 2016, the East African Community (EAC), directed the implementation of biometric permit in partner nations (Burundi, Kenya, Rwanda, South Sudan, Tanzania, and Uganda) having a one-year period for the present nationwide and public passport. The purpose is to strengthen internal security and perimeter control (Directorate of Citizenship and Immigration Control, 2012).

In consumer, biometric technology is used in the marketplace, like gate locks, monitoring application, and moveable devices (cellular phones, laptops etc.). This utilized biometrics as a

winning combination in the consumer marketplace, allowing the technology to become more widely accepted.

In financial services, biometric technology is used in protecting the money of every individual in the banks etc., such as, cash machineries with thumbprint readers presently installed around urban station to improve the clients' ease in transaction and safety.

The attack on September 11, 2001, in the United States of America (USA) cautioned governments worldwide to handle and review the safety of border control (Vakalis, 2011), thus, prompts the governments nationwide to embrace biometric passport (ePassport) for border security control.

2.3 Biometric system performance

The biometric system performance comprised of two error cases i.e., matching and acquisition errors (Ailisto, Lindholm, Mäkelä & Vildjiounaite, 2004).

2.3.1 The matching error

The matching error consists of the following:

(i) False Acceptance Rate (FAR): Mistaking biometric sample from two dissimilar individuals to be from the same individual. The FAR measure the likelihood that the biometric system accepts an impostor or it fails to turn down an unauthorized person. It's shown as the percentage of accepting an unauthorized user by the biometric system, known as False Match Rate (FMR). The formula is given below:

$$FAR(\%) = \frac{False\ accept\ number}{Number\ of\ impostors\ tested} X\ 100$$

(ii) False Reject Rate (FRR): Mistaking biometric samples from the same individual to be from two different individuals. The FRR measure the likelihood that the biometric security system turned away an already enrolled genuine user. In such case system falsely refuses to take an already enrolled person, known as False Non-Match Rate (FNMR). The formula is given below:

$$FRR(\%) = \frac{Number\ of\ rejection}{Number\ of\ users\ tested} X\ 100$$

(iii) Genuine Accept Rate (GAR): The percentage of times, an enrolled user is successfully recognized by the system. The formula is given below:

$$GAR(\%) = 100 - FRR(\%)$$

When choosing a biometric solution, there is need to discover what the FRR is at the said FAR. When a biometric solution provider claims to deliver a very low FAR, it is important to find out what is the FRR at this low FAR. In a practical scenario a low FAR and a high FRR would ensure that any unauthorized individual will not be permitted access. It would as well entail that the authorized people will induce to put their fingers along the device several times before they are granted access. So, it is just to hold a very low FAR, but recollect that if this low FAR is coming at the price of high FRR then the resolution needs to be re-assessed. Figure 2 summarized the error rates.

2.3.2 The acquisition error

The acquisition error comprised the following:

(i) Failed to capture rate (FTC): Proportion of attempts for which a biometric system is unable to see a sample of adequate quality. It's the chance that the scheme fails to discover an input given right biometric samples.

(ii) Failed to enroll rate (FTE): Probability of the user, for which the biometric system is unable to generate reference data template of enough quality. This is normally served by lower quality inputs. This includes those who, for physical or behavioral motives, are unable to give the required biometric feature (Latha & Rameshkumar, 2013).

(iii) Equal error rate (EER): The point on the curves plot of false accept rate versus false reject rate where both curves intersect.

$$EER = FAR \; where \; FAR = FRR$$

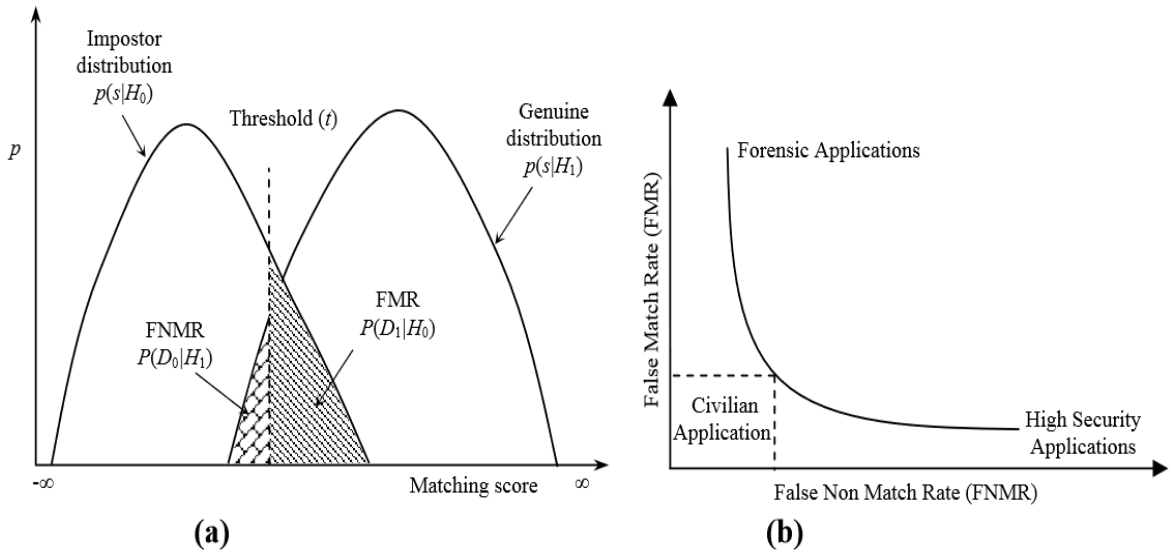


Figure 2: (a) False match rate and false non-match rate for a given threshold t (b) The curve linking FMR to FNMR (Prabhakar *et al.*, 2003)

Note: The biometric technology involved the following error rates: Failed Match Rate (FMR) and Failed Non-Match Rate (FNMR). The FMR is the proportion where the scores are larger than or equivalent to t. While the FNMR is the proportion where the scores are less than t. The curve linking FMR to FNMR is denoted as Receiver Operating Characteristics (ROC).

Jain *et al.* (2007) compared the biometric technology characters (e.g., facial, irises, and voice), it is found that fingerprint-based identification schemes are most considered than other biometric traits. Maio *et al.* (2013) stated that the verification correctness of thumbprint-based application is actual high-reaching. Table 1 summarized the comparison of the biometric characteristic.

Table 1: Comparison of biometric characteristics (H=high, M=medium, L=low)

Biometric Modalities	Universality	Uniqueness	Durability	Collectability	Performance	Acceptability	Evasion	FAR (%)	FRR (%)
DNA	H	H	H	L	H	L	L	-	-
Ear	M	M	H	M	M	H	M	-	-
Facial	H	H	L	H	M	H	L	1%	20%
Finger-print	M	H	H	M	H	M	M	0.94%	0.99%
Gait	M	L	L	H	L	H	M	-	-
Hand geometry	M	M	M	M	M	M	L	2%	2%
Iris	H	H	H	M	H	L	L	2%	2%
Keystroke	L	L	L	M	L	M	M	-	-
Palmprint	M	H	H	M	H	M	M	-	-
Retina	H	H	M	L	H	L	L	-	-
Signature	L	L	L	H	L	H	H	-	-
Voice	M	L	L	M	L	H	H	2%	10%

2.4 The vulnerability and attacks against biometric technology

Latha and Rameshkumar (2013) presented that biometric technology can be invaded by outsiders or illegal persons. The situation relates the system administrator as an insider attack or administrative frauds. Figure 3 summarized the vulnerabilities and point of attacks.

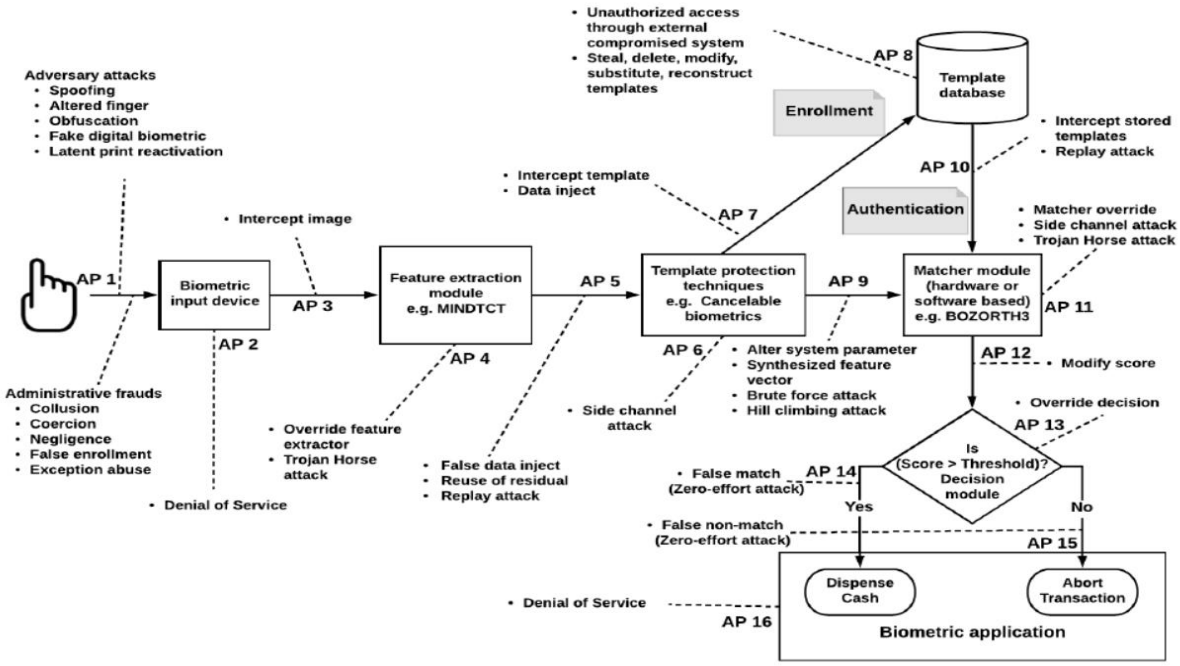


Figure 3: The vulnerabilities and attacks of the biometric technology (Yang *et al.*, 2019)

Note: AP indicates an attack point.

2.4.1 Direct and indirect attack

The attack in the technology is characterized into two, namely direct and indirect attack (Marcel, Nixon & Li, 2014). In the direct attack, an adversary executes the attacks by offering the biometric features of a registered user from the sensor interface to obtain access as an authorized user. The attacker makes the input device straightaway. Figure 3 showed the point of attacks, one, two and sixteen (Akhtar, Micheloni & Foresti, 2015).

Galbally, Cappelli, Lumini, Maltoni and Fierrez (2008) performed vulnerability of fingerprint validation in contrast to direct attack using forged thumbprints obtained from minutia templates, applying the FVC2006 DB2 database with International Organization for Standardization (ISO) minutia-based matcher. The finding indicated that 75% has direct access (Galbally *et al.*, 2010). Furthermore, Matsumoto, Yamada and Hoshino (2002) verified eleven unlike thumbprint believed coming from gummy (gelatin) thumbprints. Because an insider is indirectly involved in these types of attack. The individual can intercept the data sent over the communication channel and targets the inner factors of the biometric system to manipulate the stored data template. Figure 3 indicated the attack point AP 1, AP 2, and AP 16.

2.4.2 Repudiation

The repudiation is the denial or refusal of the approved system. The attacker denies having accessed the application. Figure 3 specified the attack point 16.

2.4.3 Coercion

The coercion is the legal user unknowingly being instructed by impostor to allow entree to the biometric application (Nandakumar, Jain & Nagar, 2008; Ratha, Connell & Bolle, 2001). The impostor utilizes the biometric application with the user's biometric data for monetary transactions.

2.4.4 Administrative fraud

The administrative fraud happens when user assist putting or revealing secret information of the organization. It involves the following:

(i) Collusion: Where administrator is an impostor to change the access rights of an allowed operator.
(ii) Failed membership: Where administrator helps enroll the impostor into the application. The decision maker is pleased with a huge kickback for the unlawful enrolment for first appearance.
(iii) Oversight: Where administrator aid the invader entree as a registered user. Changes the verge to an inferior rate so the opponent can get the advantage.

2.4.5 Sensor attacks

In the sensor attacks, Latha and Rameshkumar (2013) indicated that the intruder present fake fingerprint to the sensor to produce lawful image. The impostor puts on face mask cause denial-of-service (Pratiba & Shobha, 2013).

Kang, Lee, Kim, Shin and Kim (2003) applied a number of fingerprint sensors for testing and examine if the sensors can eliminate a fake fingerprint film. The results exhibited that the fake finger films are assumed by most of the tested sensors. Schuckers (2002) added eleven dissimilar fingerprints-based verification systems to forge fingerprint films, the results shown that more than 67% probability forged fingerprint films are enrolled in the systems. Kim (2017) implemented descriptor image to hold fingerprint liveness detection. It is revealed that

forged fingerprints generated no match. With smart phones, care must be taken against thumbprint scamming (Yang, Hu, Fernandes, Sivaraman & Wu, 2016). The suggested is liveness detection such as the software-based solutions and the hardware-based solutions (Schuckers, 2002; Roberts, 2007; Yoon, Feng & Jain, 2012; Yang *et al.,* 2019).

2.4.6 Character extractor attacks

The attack involved:

Override character extractor: This is where, the attacker replaces the characters fearlessly (Kamaldeep, 2011; Ratha *et al.,* 2001; Ross, Nandakumar & Jain, 2008). The Trojan horse extracts user's fingerprint samples, then send it to the impostor. The countermeasure is to use software detection mechanism to spot the Trojan horse (Yoon *et al.,* 2012).

2.4.7 Attack on database template

The invader marks the storage record straightaway via a visibly conceded application to mount denial-of-service (Arjunwadkar *et al.,* 2012; Habibu & Sam, 2018; Poongodi & Betty, 2014). Figure 3 characterized point eight attack.

Study by Gobi and Kannan (2014) indicated that, the storage database is the most area targeted by impostor. Because the biometric data template can be infringed and revised (Xi & Hu, 2010). Brindha and Natarajan (2012) pointed that, the biometric data in the database can be replaced by an invader's pattern to attain illegal access to biometric application. Mwema, Kimwele and Kimani (2015) and Raju, Vidyasree and Madhavi (2014) observed a bluffing attack as one of the problems in the biometric data template storage.

Manvjeet and Sanjeev (2010) argued that, the possible exploitation of biometric data templates can be used for other purpose than the original planned aim, because the data can be used for extra aim. Therefore, underprivileged to person's consent. For example, thumbprint obtained can be utilized to search for an illegal thumbprint for wrong check in financial sector (Prabhakar *et al.*, 2003).

The four vulnerability attacks in database templates are:

(i) The template being replaced by an invader's template to obtain illegal access.

(ii) The physical spoof can be produced or generated from the template to gain illegal access to the organization data as well as other schemes that employ similar biometric feature.
(iii) The stolen template can be replayed or reiterated to the matcher to gain illicit access.
(iv) The template can be used for cross-matching across dissimilar database records.

Li and Kot (2011) presented a secrecy security measure. In their study, user's identity is concealed. Elkamchouchi *et al.* (2018) recommended a technique of cryptography utilizing the image as a public key and arbitrary numbers as a secret key to compute the pixel. Liu, Li, Cao and Chen (2017) considered cryptographic system of secret transmission to encode a decoded message. The authors suggested cancellable biometrics and biometric cryptosystem to protect the template (Jain, Nandakumar & Nagar, 2008). An online platform, EvaBio, for the security assessment is discussed (El-Abed, Lacharme & Rosenberger, 2012). Table 2 presented the vulnerabilities and threats of the biometric technology.

Table 2: The possible attacks with reference to Fig. 3 attack point (Yang *et al.*, 2019)

Attack point	**Target component**	**Possible attacks**	**Countermeasures**	**References**
1	Biometric input device	Adversary attacks and Administrative frauds	Liveness detection, Trial/reply	Marasco and Ross (2015); Hadid, Evans, Marcel, and Fierrez, (2015)
2	Biometric input device	Denial of service	Rugged devices	Jain *et al.* (2008)
3	Communication path between sensor and feature extraction	Fingerprint image intercept	Transmit data over an encrypted path/secure channel	Jain *et al.* (2008)
4	Character extractor module	Trojan horse attack, Override feature extractor	Transmit data over an encrypted path/secure channel	Jain *et al.* (2008)
5	Communication amongst character extractor and template safety methods	Replay attacks	Trial/reply based application.	Shelton *et al.* (2012)
6	Template protection techniques	Side channel attacks	Masking, designing ICs with active shield	Dürmuth, Oswald, and Pastewka, (2016)
7	Communication amongst character extractor and template safety methods and template database	pattern capture, Data hijack	Usage of robust confirmed procedures	Ross, Shah, and Jain. (2005)
8	Template database	Steal, delete, change, replace template	Toughened server, entree controls, Store encrypted templates	Jain *et al.* (2008); Jain, Ross, and Uludag (2005)
9	Communiqué amongst template safety techniques and matcher	Hill-climbing attack, Brute force attack	Timeout/lock out policies	Tams (2013)
10	Communication amongst template database and matcher	Replay attacks	Apply Timestamps	Roberts (2007)
11	Matched	Side channel attack, Trojan horse attack	Covering, Code signing	Dürmuth *et al.* (2016)

Attack point	Target component	Possible attacks	Countermeasures	References
12	Communication path between matcher and decision module	Modify score	Mutual authentication between matcher and decision module	Jain *et al.* (2008)
13	Decision module	Override decision	Code signing	Roberts (2007)
14	Communication amongst decision module and biometric application	Zero-effort attack (False match error)	Design robust matcher	Tams (2013); Jain, Ross, and Pankanti (2006)
15	Communication amongst decision module and biometric application	Zero-effort attempt (False nonmatch error)	Design robust matcher	Jain *et al.* (2006)
16	Biometric application (e.g., cash dispenser)	Denial of service attack	CCTV monitoring, deploy security guards	Jain *et al.* (2008), Roberts (2007)

2.5 Privacy and security risks of the biometric technology

Despite the rapidly growing number of biometric applications, in areas such as bodily and physical access control, attendance time, border control, identity documents, financial banking, a lot of potential privacy and security risks continues to draw more attention. For instance, the privacy and security issue discussed below.

2.5.1 Privacy issue

Ang, Safavi-Naini and McAven (2005) indicated that an attack in biometric technology targets the data access at the storage database. Simoens, Bringer, Chabanne and Seys (2012) distinguished distress as follows:

(i) Biometric Sample Recovery: Where an adversary determines a new template predictable by the storage server.
(ii) Biometric reference recovery: An unauthorized party (adversary) succeeds in acquiring the biometric data template (plaintext) reference from the database. This is the greatest destructive privacy threat, because an attacker can obatin unlawful biometric data template contact to the application sample gathered.

Pagnin and Mitrokotsa (2017) indicated the most provoking challenges in the biometric authentication system as follows:

(i) The refusal of impersonation attacks.
(ii) The inevitability of biometric data templates.
(iii) Guarantee that individual data remains secret.

Mordini (2008) presented that the central recording to biometric data is vital to privacy matter, because the stored information can be copied or interfered. The sensitive data of the individual's character and health can be exposed. Consequently, soft biometrics need to be investigated thoroughly as a way to manage individuals' information.

Pagnin and Mitrokotsa (2017) suggested that, the countermeasures to combat the secrecy fear is through the use of the cancellable biometrics and bio-hashing (Topcu, Karabat, Azadmanesh & Erdogan, 2016).

2.5.2 Security issue

Nandakumar and Jain (2008) pointed out that the greatest security problem of the biometric technology is the input interface in offering a false biometric representative, such as voice, face, signature in which an impostor stages a false biometric trait at the sensor machine. The impostor can exchange a fake biometric data with a genuine one during the verification context (Jain, Nandakumar & Nagar, 2013). The security vulnerability of biometric is instigated by the impersonator exploiting the biometric traits at the sensor machine interface (Jain *et al.*, 2008; Nagar, Nandakumar & Jain, 2012; Phillips *et al.*, 2007; Przybocki & Martin, 2004; Wilson *et al.*, 2004). The countermeasure is to provide a liveness recognition technique as well as system designers to install security surveillance.

2.5.3 Weakness of the biometric technology

The weakness of the biometric technology includes:

(i) The biometric data aren't private. Because hackers can acquire the biometric traits such as fingerprint, facial, voices, iris etc., anywhere in restaurants, supermarkets, workshops, conferences. With fingerprint recognition you leave fingerprints everywhere you go. With voice recognition, someone is recording your voice. Essentially, places you visit records and saves your image in its database to identify

you and analyze your buying habits. Some images are taken without owners' consent for commercial purposes. All it takes is for a hacker to breach any of those databases to leak and steal your biometric identification. Therefore, Personal Identifiable Information (PII) needs to have access control in place to protect one from identity theft.

(ii) The biometric data template in the database are hackable, once an impostor has an image of someone's fingerprint, facial, or iris, they can easily gain access to the accounts. The Apple's TouchID was broadly accepted as a biometric advancement, famous hacker Jan Krissler was able to hack the technology just a day after the iPhone was released. Likewise, researchers from the Chaos Computer Club (CCC) created fake fingers to unlock iPhones.

(iii) Since biometric technology reveals part of a user's identity, if stolen, it can be used to forge legal documents, passports, or criminal records, which can do more damage than a stolen credit card number. Biometric companies are aware of these errors in the technology and should aim to improve identification. Therefore, multi-factor authentication can help reduce the fraud.

2.6 Biometric template protection measures

Jain *et al.* (2005) explained that the biometric data template protection ensures that, data are not revealed or replayed and makes it hard for an attacker to reverse engineer the stored data (Pratiba & Shobha, 2013; Radha & Karthikeyan, 2010).

Busch (2012) categorized the ISO/IEC 24 745 standard into three i.e., non-invertibility, revocability and unlikeable (Al-Saggaf & Acharya, 2013; Nandakumar & Jain, 2015). Tigga and Wanjari (2013) classified the biometric template measures into two (2) categories i.e., hardware and software-based. The hardware-based method comprised of the smart cards or match-on-card. While the software-based keeps a reviewed disclosed data. Because, users carry the card every other time.

Despite the hardware and software-based protection template, Nandakumar and Jain (2015), Sandhya, Prasad and Chillarige (2016) and Simoens *et al.* (2012), broadly categorized the biometric template protection further into feature transformation and biometric cryptosystem. The feature conversion method is further categorized as a salting-based method and non-

invertible method. Whereas the biometric cryptosystem approach is categorized as key binding and key generation method. Figure 4 presented the various stages of the protection techniques.

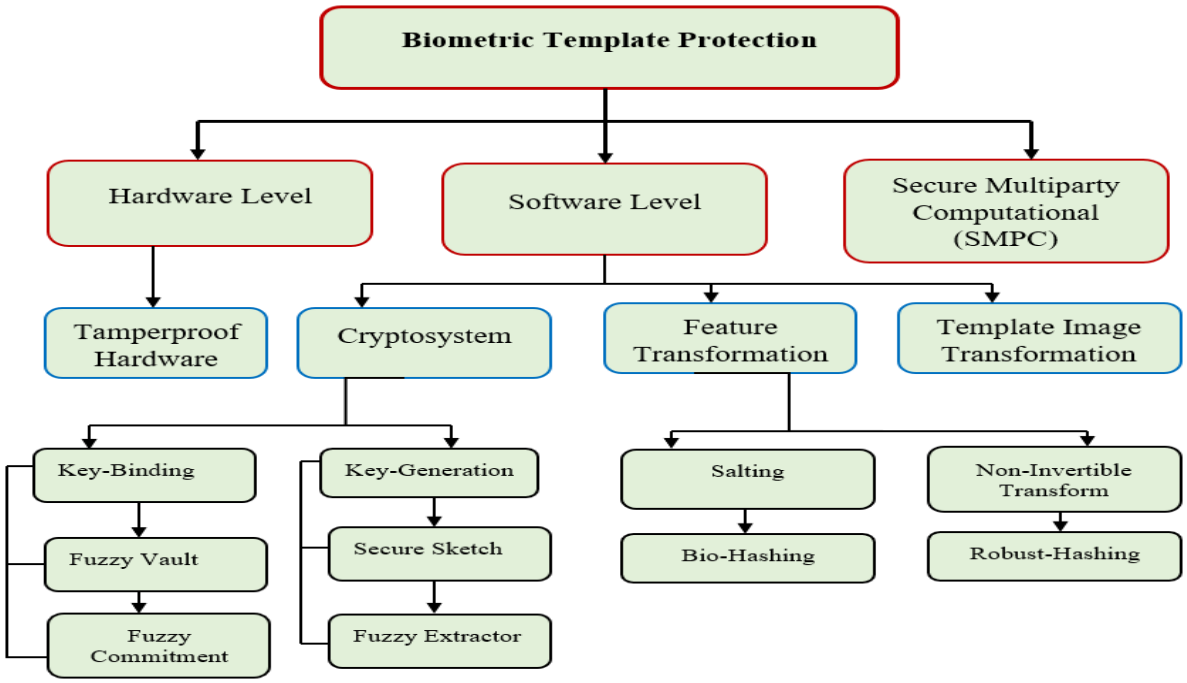


Figure 4: Categorization of the biometric template protection scheme (Joshi, Mazumdar & Dey, 2018)

2.6.1 Hardware-based level

In the hardware level safety, the data templates are achieved and rendered to avoid interception and interfering of patterns. A tamper-proof prohibits an invader from infringement into the system, like matcher, to steal a private key and thus prevent illegal entree. The Trusted Platform Module (TPM) is developed by Trusted Computing Group (TCG) as platform that comprises extra hardware and software to rise the security level of Information Technology (IT) systems (Alshar'e, Zin, Sulaiman & Mokhtar, 2015).

2.6.2 Software-based level

In the software level, it mostly focused in the storage of the data template kept in the database in a coded form. This makes it very difficult for an invader to break through the enciphered

key. The application involved the cryptosystems, data template creation utilizing character conversions.

2.6.3 The feature transformation

Pratiba and Shobha (2013) indicated that the template in feature transformation is distorted using the user's password during the enrolment and the same password in the transformed query before being fitted with the transformed template. The transformed function is gained through the biometric template. Then saved in the database. Christian and Christoph (2012) argued that, the element of the transformed function is acquired from an arbitrary mystery key or password. And so, the same transformed function is localized in the feature query and matched against the transformed template. Gaddam and Lal (2010) discussed various transformation functions available such as, bio-hashing (Topcu, Erdogan, Karabat & Yanikoglu, 2013), cancellable biometric (Patel, Ratha & Chellappa, 2015) and biometric salting (Jain *et al.*, 2008).

(i) The bio-hashing

Armoogum and Oozeer (2016) and Mwema *et al.* (2015) indicated that the bio hashing is transformed and defined with a secret key only known to the user. The key is securely hidden away and recalled for subsequent authentication this increases entropy of biometric templates, and deters adversary attacks. The biometric data is used to compute a binarized key of 80 bit keys with 0.93% false rejection rate (Radha & Karthikeyan, 2010). The key can be used in smartcard or Universal Serial Bus (USB) tokens (Gobi & Kannan, 2014).

The major drawback of bio-hashing is the reduced routine where the genuine token is recovered and delivered by a rival claiming to be a lawful operator (Minakshi, RupKumar, Deepjyoti & Rupam, 2012). Jin, Ling and Goh (2004) presented two-factor authentication technique for bio-hashing. The analysis done by Nagar, Nandakumar and Jain (2010) indicated that bio-hashing is susceptible to interference since it is quite easy to acquire unique pattern.

(ii) Cancelable biometrics

Ratha, Connell and Bolle (2001) pointed that, in cancelable biometrics, the original data template is rendered by non-invertible conversion in the starting point and the sample data in the authentication level. Ratha, Chikkerur, Connell and Bolle (2007) introduced three

different transformation functions. The suggested transformed function deliberately misrepresents the original features, making it complex to retrieve raw data template.

Yang, Jiang and Kot (2009) formed cancelable templates using nearby and universal characteristics. The nearby features comprised of the reserved and comparative viewpoints amongst minutiae sets, while universal characters comprised of alignment and ridge frequency. Yang, Hu, Wang and Wu (2018) suggested a multimodal cancelable biometric system that fuses fingerprint features and finger-vein features to achieve better recognition accuracy and higher security.

Dwivedi and Dey (2019) suggested a hybrid combination system to assimilate cancelable fingerprint and iris modalities to lessen restrictions in each person modality. Investigational effects exhibit high performance improvement over their unimodal counterpart. Unlike passwords, PINs and access codes, biometric template can never be replaced by youngster if compromised.

To circumvent these risks, cancellable biometrics are introduced where biometric templates can be cancelled and substituted (Patel *et al.,* 2015; Radha & Karthikeyan, 2010). The cancelable biometrics resolves secrecy-related applications as it averts the system to stash away the unique biometric characters of the operator.

According to Rathgeb and Uhl (2011) cancelable biometrics has got its challenges, if transformed biometric data is compromised, transformation parameter changes to deter adversaries from tracing and cross-matching users' templates, if transformational parameter are known to hackers, it's insecure, because it reduces recognition accuracy due to the high variance brought about by the distorted data when transformation is applied on users' biometric data (Du, Yang & Zhou., 2011).

(iii) Biometric salting

Sandhya *et al.* (2016) indicated that a user-specific data is linked with the biometric data to obtain the partial version. Depending on the exterior supplementary data, the technique is revocable only by switching the word. This evokes a grave security issue, because the user-specific data can be stolen or compromised. In the event of non-invertible transformation, the biometric sample is distorted by giving a one-way non-invertible role, the parameter of the transformation is altered to provide adaptable templates. The translation is performed through sign area or in feature field. Patel *et al.* (2015) pointed out that, the benefit of the non-

invertible convert is that the fraud can't rebuild the unique biometric data even if the converts are approved, non-invertible transformation increases the performance reduction due to information loss and difficulty in arrangement of the data templates.

2.6.4 Biometric cryptosystem

Supriya and Manjunatha (2014) stated that the cryptosystem is encoded using an encoded key derived from a password. The stored data is decrypted using the matching decrypted key correspond to the captured query for the authentication. The data is kept in the helper data to prevent expose of any important message in the biometric template. Meanwhile the encode key can be mixed out after generating the secure template, thus, an attacker can't replace or exchange the existing encrypted template even if the decryption key is stolen.

The cryptosystem is divided into stages i.e., cryptographic of secret key from a data template (Kholmatov & Yanikoglu, 2006). A biometric cryptosystem output a key by either attaching it with the biometric features, such as Fuzzy Commitment (FC) (Ari-Juels & Wattenberg, 1999). Fuzzy Vault (FV) (A-Juels & Sudan, 2002; Uludag, Pankanti & Jain, 2005). Or straightaway creating the key from the biometric characters, for instance, Fuzzy Extractor (FE) (Dodis, Reyzin & Smith, 2004).

(i) Key binding

In a key binding, the key is combined with assistant data in the registration stage (Imamverdiyev *et al.,* 2013). Figure 5 summarized the basic concept of biometric key binding. The key binding involves the following: Fuzzy Vault and Fuzzy Commitment (Billeb, Rathgeb, Reininger, Kasper & Busch, 2015).

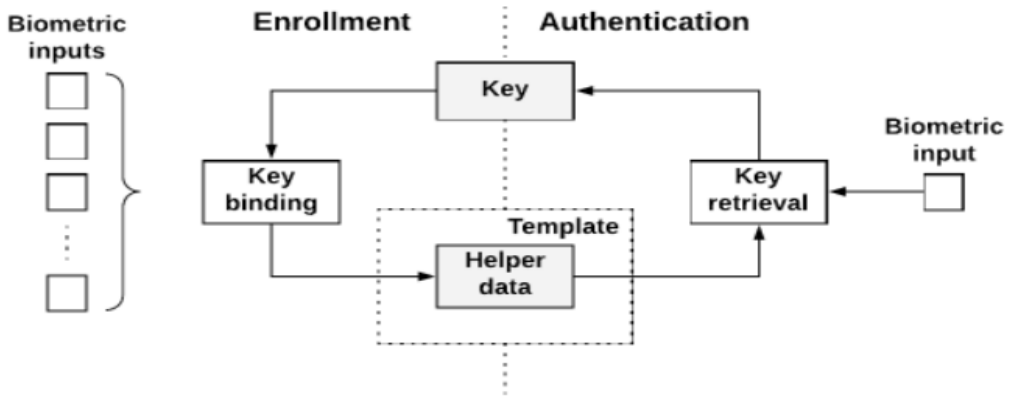


Figure 5: Basic concept of biometric key binding (Joshi *et al.*, 2018)

(ii) Fuzzy vault

According to Geetika (2013) a biometric FV is used for protecting private key, releasing them only when the legitimate users enter the correct biometric data. It encrypts the secret information, then decrypt it using a fuzzy unordered set of genuine and half points.

Meenakshi and Padmavathi (2010) revealed that fuzzy vault eliminates key management problem found in the practical cryptosystem. Hooda and Gupta (2013) indicated that fuzzy vault is prone to the following limitations, difficulty in revoking a compromised vault, which is prone to cross-matching of biometric templates across databases. An attacker can easily stage attack after statistically analyzing points in the vault. It's possible for an attacker to replace the original biometric features with fake one, thus, beating vault authentication. If the unique template of the legitimate user is temporarily exposed, the attacker can glean the template during the exposure.

(iii) Fuzzy commitment

Jeny and Jangid (2013) indicated that the biometric traits in fuzzy commitment are characterized in binary vector or uniform random key of length 1 bit, generated and used to fully index an n-bit code of error correcting code. In which a sketch extracted is stored in a database. Geethanjali, Thamaraiselvi and Priyadharshini (2012) compared the different between fuzzy commitment and fuzzy vault. They indicated that, fuzzy commitment is characterized as binary vectors, divided into various segments where each segment is securely separated. While in fuzzy vault the biometric trait is given as a set of securely hidden data (Al-Saggaf & Acharya 2013; Schmitt & Jordaan, 2013).

Liu and Zhao (2017) used 11 minimum number points to protect the thumbprint templates and kept them in encoded form. Thumbprint matching is conducted in the encoded field and validation is positive only when the query thumbprint is close to the fingerprint template (Cappelli, Ferrara & Maltoni, 2010).

2.7 Techniques to secure data storage

The data in the databases are the greatest and harmful attacks that cause serious consequences for users. The biometric information is usually registered and compared with the stored information in the confirmation phase. There are serious fears of users with utilization of the biometric data. Because an impostor can hijack the biometric information in the storage to

attain unlawful access to the biometric system. To secure the biometric data template in the database, a range of techniques has been proposed by different scholars to secure biometric data template and database (Mm & Gr, 2017).

Jain *et al.* (2005) and Emmanuel *et al.* (2016) suggested the shorthand to hide the raw biometric data whose purpose is to transfer the data. The method prevented a skimmer from understanding delicate information (Patel *et al.* 2015). This condensed the template conceded and resolved the genuine replacement of a secrecy issues for matching against distorted vector, as well as, averts the application from keeping the new biometric characters of the user.

Pratiba and Shobha (2013) anticipated a watermarking method to watermark the data in the biometric template database. Setting aside the honesty of the substance to be shown, when recovered for identical. The pixel rate skins the watermark data (Malhotra & Kant, 2013). In case an impostor attempts to substitute the safe biometric data template, the system signal from the server for wrong trials attempts (Anitha, Rao, Rajasekhar & Krishna, 2017).

Nandakumar and Jain (2015) proposed the fuzzy vault design using thumbprint and iris. The study revealed that multi-biometric vault in thumbprints and iris achieved 98.2% of the GAR at 0.01% FAR. The equivalent GAR rate of the individual's iris and thumbprints vaults is 88% and 78.8% respectively. The safety of the system is 41 bits and that of the thumbprint and iris has provided 49 bits of security (Gomez-Barrero, Maiorana, Galbally, Campisi & Fierrez, 2017; Khan, Akbar, Shahzad, Farooq & Khan, 2015).

Ashish and Sinha (2016) suggested the utilization of string re-arrangement to ease the safety of the template database. The biometric information is encoded and castoff after creating the easy template. During the check, the stored information is decoded using the private key and checked contrary to the token request. The obstruction to the encoded-based strategy, is the unprotected key controller, which showed the decoded private key to the machine for each certification. The benefit is the matching process hired for sustaining the similar correctness (Rathgeb, Gomez-Barrero, Busch, Galbally & Fierrez, 2015; Simoens *et al.*, 2012).

Manvjeet and Sanjeev (2010) suggested encryption-decryption algorithm to secure the fingerprint image incorporated with a password. The password involved the mathematical value of any length, and image of any size using polynomial function d^x where $d^x = d1x5 + d2x4 + d3x3 + d4x2 + d5x1 + d6x$ (AlTarawneh, Woo & Dlay, 2008). The

effects were studied on a database containing 50 images of fingerprint templates, 50 images of any biometric traits or whatever other information needed to decode or decrypt and a word needed for private key generation. The findings showed that the developed technique gives 96% security when 50 images of biometric traits are encrypted and decrypted with 50 different passwords. And 100% security when the 50 images of biometric traits are encrypted and decrypted by using one image of fingerprint template and 50 different passwords.

Nagar *et al.* (2012) proposed liveness detection mechanism in preventing the outbreaks attack. The authors implemented liveness detection using software and hardware. The extra hardware obtained life signs for recognition, for instance, face to face movement. The disadvantage is that, more hardware is required that makes it extremely expensive (Panigrahy, Jena, Korra & Jena, 2009). To address the secrecy and security issue of an individual's biometric data, a fingerprint and facial image are integrated using the cryptographic module based on the Fernet keys instance of the encryption-decryption algorithm to protect the biometric database. In this, the identity of an individual is firmly protected.

In general, the study introduced an overview of the biometric operation mechanism and its performance and then went on to identify the vulnerabilities and attacks as well as privacy-security issues and the weakness. It is realized that, most of the impostors targeted the biometric data template in the database. The biometric data template in the database can be hacked, once an impostor has an image of someone's fingerprint, facial, or iris. The impostor can easily gain access to their accounts, reveals part of a user's identity, and if stolen, it can be used to forge legal documents, passports, or criminal records, which can do more damage than a stolen credit card number.

However, several methods were discussed, for instance, the cancelable biometrics to enhance the trustworthiness of the biometric data template, the bio-hashing to transform and define data with a secret key only known to the user, biometric salting to define user-specific data linked with the biometric data, fuzzy vault for protecting private key and release them once the legitimate users enters the correct biometric data and fuzzy commitment to generate binary vector or uniform random key of length 1 bit. It was discovered that, there is no totally foolproof of security scheme that guaranteed the protection of the biometric data template in the database. Therefore, no biometric system is optimal. The determination as to which biometric technology is to be used should be prepared on the foundation of the operation and

the degree of protection required. The research, therefore, addressed the common weakness related to:

(i) Privacy and security risks, where biometric information in the database is retrieved without user's awareness.
(ii) Unauthorized thirdy party, succeeding in recovering the plaintext reference of biometric data template in the database.
(iii) Users traceability, where an adversary can trace user's authentication and tries to access the biometric data in the database system.

The study, therefore, suggested the encryption-decryption algorithm linking to the cryptographic module incorporating the Fernet keys instance. The cryptographic module integrated the biometric traits (fingerprint and facial image) with persons biodata, to produce an encrypted byte and a text file. These files are securely saved in the database incorporated with Twilio short message service (SMS) message. The Twilio SMS message is auto-generated directly from the database to alerts the user and the officer in circumstance an attacker attempts to access the database, it can block the attacker from unauthorized access and cross verify the attacker based on the validation of the ownership, i.e., authentication code. With this approach, users biometric data is more secured and harder for an impostor to guess the key mixtures and suitable for use in many biometric software applications.

CHAPTER THREE

MATERIALS AND METHODS

3.1 Introduction

This chapter introduced the most substantial component of any research work, because it described the attainment questions. The determination of the learning is to create an impression to individual skills and worries of the application system in Uganda and to develop secured procedure for protecting the biometric data in the storage. The chapter defined study design, population and sample technique, data collection, case study and documentation, data analysis, validity and reliability as well as ethical consideration.

3.2 Study design

The study adopted investigation tactic since it's flexible for online inquiries. Coded requests are offered through surveys. The initial survey is introduced, explained and ideas given by experts. The questions are altered, formulated and tested out via a few samples (pilot-trial). The results of the pre-trials are utilized to remove, redesign new questionnaires.

3.3 Population and sampling procedure

The respondents surveyed are persons holding travel permits and officers at migration currently processing the permits exercise. The stratified random sample is utilized to draw the target goal. The formula below is used to draw the subgroup or strata within the population and to ensure that the presence of the key subgroup is selected, makes it more precise, accurate and better estimate of the population. The formula $S = \frac{X^2 . P(1-P)}{d^2}$ is deployed for the sample size (Shalabh, 2014). By using this approach to find the sample size, it is anticipated that the degree of bias can be fixed and the measurements of sampling error becomes low. The method selected account for the extrapolation of the results from the study of the whole population.

3.4 Data collection

The research deployed a qualitative and quantitative questionnaire that captured data pertinent to the research's objective in the four regions of Uganda: Central, Eastern, Northern and Western. The questions involved four levels: social-demographic characteristic of the

respondents, like the respondent's age, gender, skill level and type of respondents. The second, attributed to the influences affecting individuals worry of biometric technology. Third, safety intimidations of the technology. Finally, suggested countermeasure. Unlimited questionnaires are utilized for the study. The closed questions are used to collect data to avoid ambiguity data in situations of non-conforming selected choices of the questions given to the answerers. Other reasons are, to get qualified focused responses over which study questions can be replied. Meanwhile the survey is automatically dispersed, it confined the participants to response the questions accurately and with less time-consuming as related to the open survey.

3.5 The case studies and documentation

The case study and documentation review approach were used for the public available documents. The documents included the mission statements, annual reports, guides and strategic plans as well as personal documents such as the Journals, blogs, event reports, newspapers and physical evidence like brochures, posters, reference works and training materials. The case study and document analysis are an effective and efficient way to collect data because they allow revealing a deeper understanding of the existing literature because they are clearer, more accessible, more reliable, less expensive and more cost-effective than other methods (Bowen, 2009; O'Leary, 2004)

3.6 Data analysis

The study used RStudio and the Statistical package for social sciences (SPSS) version 20.000 for data analysis. The SPSS enabled to extract data from the table. While RStudio was used to manipulate the statistical modeling and graphics. A chi-square value below 0.050 was used to measure the significance differences based on chi-square test. The investigator tabulated the raw information gathered from the participants utilizing the surveys to describe the graphs. This is suitable in that, the description of similar answers utilized the same tactic of expressive study and to twist the raw facts into important data for policymaking and recommendation. Beside analysis, the investigator deployed new tactic of encryption-decryption algorithm using the design pattern of MVT as solution to secure the biometric data in database. The algorithm is based on the cryptographic module of Fernet keys instance, where two Fernet keys are combined to generate a multiFernet key for the encryption. The

software's installed are Jinja2, Wtforms, SQLAlchemy, Cryptography, Twilio SMS using a python flask as the web development platform.

3.7 Validity and reliability

The validity is the degree to which an assessment measures what it says to measure (Stake, 2010; Golafshani, 2003). It is extremely important that an evaluation is valid so that the results are applied and interpreted correctly. According to Golafshani (2003) reliability is the degree of agreement of results over time. The results are said to be reliable if similar results can be simulated using the same methodology, then it is known that the research tools are reliable. To ensure the validity and reliability of the study, data were collected using various techniques (interviews, case study, documentation analysis, direct observation, participant observation, and experiments) from different expertise (Directorate of migration officers, Information and Communication Technology (ICT) experts, and receptionists). This aided to obtain information from multiple angles and increased the legality of the information required.

3.8 Ethical consideration

The investigator obtained a permission from the School of CoCSE at the NM-AIST Arusha, Tanzania and the MU administration office Arua, Uganda who addressed the letter directly to the Minister of internal affairs office for conducting the study in different regions/centers of the migrations and border controls (Appendix 3 and 4).

The investigator requested for the permission to use the research instruments such as cameras during observation, recording during the interview, photos and narrations from respondents for the study purpose. The researcher adhered to the ethical principles that included respect for the privacy and the person, honesty, integrity and confidentiality. According to Berg (2008), ensuring confidentiality is critical if the researcher expects to get truthful and free-flowing discussions during the interview.

CHAPTER FOUR

RESULTS AND DISCUSSION

4.1 Introduction

In this section, results from the survey were conducted. The discussion of the analysis based on users' concerns of biometric technology is presented. The encryption-decryption algorithm implemented to secure the biometric data template in the database are explained in detail. The graphical illustration of the respondents is presented to infer the results in a more serious manner.

4.2 Social demography characteristic

This section sought to determine the participant's conceptions about the general population concerning biometric technology usage and the wider knowledge of experience. The details included gender, age and biometric feature experience as well as the security of the biometric data.

Three-hundred-and-eighty-four (n=384) participants are documented holders, while thirty-three (n=33) respondents are issuance officers. The 74% of the participants are male and 26% are female respectively for the passport holders. While 69.7% and 30.3% are male and female equally for the issuance officer. Sixty-five percent (65%) are mostly of the old year, above the age of 30 and 35% are between the age of 21 and 30. The motive behind this, is to take an impression of the general public about the utilization of the biometric application.

The foremost participants are from the university communal, hold formal prerequisite higher than Advanced level for passport holders (BSc., MSc. and PhD) and officers at the district centers in the event of issuance officers. Forty-point-six percent (40.6%) are undergraduates, 37.2% are training staff and 22.1% are workers. This is to evaluate if the participants are mindful and knew about the new technology applied in the biometric passport.

No substantial variations in participants' features amongst the three groups were observed (chi-square value = 0.002). The wider information and expertise in biometric application systems used are analyzed. The purpose is to understand if the biometric application used had an influence on the acceptance of the users. The 48.5% and 53% of the participants have wide

range of skills in fingerprint, 31.3% and 36% for face image, 9% and 4% for iris, 5% and 3% for palm image, lastly six-point-two-percent (6.2%) and four-percent (4%) for voice.

The participants indicated the usage of the biometric technology in the workstation, countrywide registration among others (NIRA-Uganda, 2015). Furthermore, the findings showed that despite this high percentage of respondents with a broader expertise knowledge, 69.3% of the respondents' agreed that, most organizations are using biometric technology for security reasons. Thirty-point-seven percent (30.7%) disagree with the statement, that the information can be invaded and misrepresented by an impostor.

So, a need for person's mindfulness about the safety and secrecy of the information they provide throughout the numerous registrations in everyday events. The results from the analysis are summarized as shown in Fig. 6.

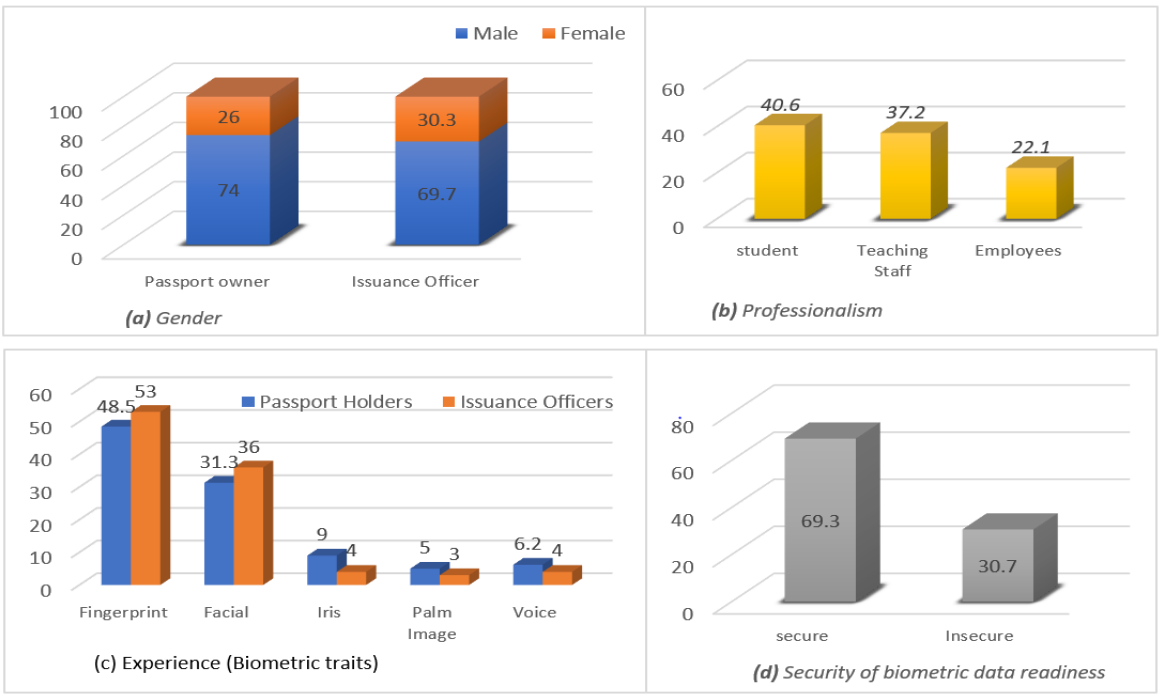


Figure 6**:** The social demography features of the participants (a) Gender, (b) Professionalism, (c) Experience on biometric features, (d) Security of biometric

4.3 Factors determining the acceptance of the biometric application

This segment showed a link amongst the intellects and moods of the participants about the insight of the technology application utilization. It assists the scholar to ascertain the foremost worries overdue the use of the biometric technology in order to instruct the expert in

understanding the preference of the overall community. The 30.2% of the participants' accepted that the technology help in securing the person's data from scams. Nonetheless, seventeen-point-four percent (17.4%) disagreed with the declaration citing that, the technology cannot help in securing frauds and crimes, because the data can be manipulated. Also, 2.4% are unbiassed (neither agreed nor disagreed). Although there is a various observation of the participants, those who agreed to adopt it, indicated the importance ration in contrast to crime and fraud, while those who strongly distressed saying the technology cannot aid in stopping fraud and crime against humankind.

The respondents were questioned on the protection provided by the use of biometric passports. The 28% disagreed with the statement. They indicated that this technology cannot help offer any security, because the protective equipment can fail to detect against terrorist act. However, 37.4% accepted that the technology offers solid validation and enhance safety at the border point. Twelve-point-two percent (12.2%) are unbiassed (neither agreed nor disagreed).

Furthermore, participants were questioned of the technology utilized, forty-three-point-five percent (43.5%) strongly accepted the technology as a way to prevent and validate the holidaymakers at the border entry. The 11.2% strongly disagreed, considered it as a hinderer. Hence, creating a fortune for a terrorist to invade the system. Fifty-six-point-five percent (56.5%) believed that biometric technology is employed as surveillance to constantly monitor crimes against mankind which can help forestall a terrorist onslaught. Seven-point-six percent (7.6%) disagreed with the statement.

Given the knowledge of the respondents about the technology, 41.2% of the participants concurred with the statement. Because the biometric data is kept on the passports without the holder's willingness. While 30% did not agree and 7.4% are neutral.

Therefore, the officers and system operators need to make up-to-date recommendation on the acceptance of the technology to ensure safety of employer's data from frauds. The results for the study are illustrated in Fig. 7.

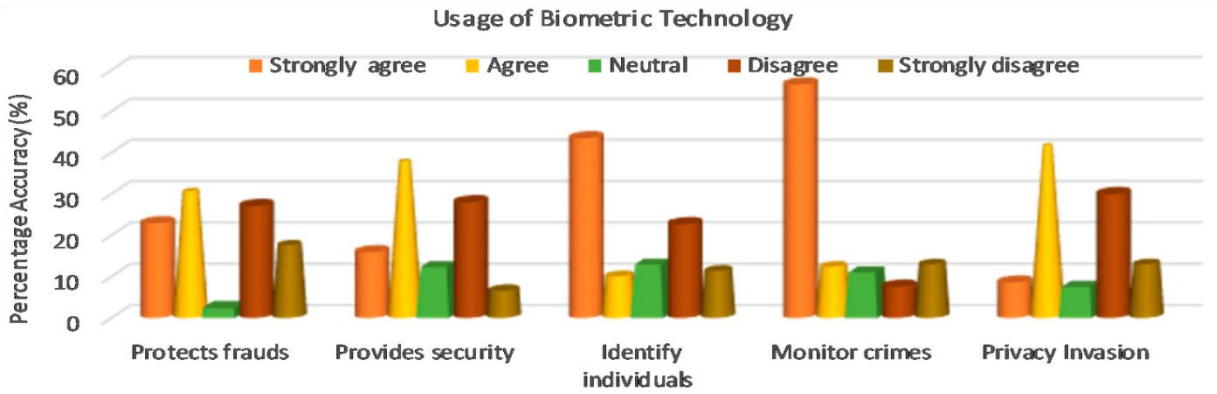


Figure 7**:** Utilization of the biometric passport technology

4.4 The biometric data secrecy

A considerable issue of data secrecy and safety compliance is examined on the five-Likert-point, ranging from 'Strongly agree' to 'Strongly disagree'. Information saving is done in the range of 1 to 5. The weighted average and statistical numbering of p-value beneath 0.050 are estimated. The 80.2% of the participants presented that users' data cannot be disclosed deprived of the holders' consent, because individual information is of vital economic worth. Thus, one demands to identify whom to share the datum with and what is to be done with the data. The statistic rate attained is 0.000 and a weighted average of 1.200. Therefore, the participants' declaration is acknowledged.

Additionally, 57.8% of the participants strongly agreed that individual information should be held confidential, because individual data is private and must be secured. Individuals should determine to observe the rules against their own information (Singh, 2014). Through any data placed available in a community forum, individual cannot assume it's secret or protection. The chi-square value attained is 0.000 and a weighted average of 1.48%. Hence statistically substantial.

The possible misuses of novel knowledge by biometric offenders are explained for validation purpose. The 64.8% of the participants strongly accepted that novel technologies can be harmed and broken by crooks, since identity theft, counterfeit and fraudster are the actual cause. While biometrics technologies aid in security in contrast to the occurrences, the possible abuse is noticeable. Anyone unidentified can involve themselves with outsiders and exchange information records. Besides, a good figure of workers does not entirely identify the threats related to the utilization of new biometric technology. One needs to know that a

stolen biometric data cannot be cancelled. The figure value attained is 0.001 and the weighted average equals to 1.510. Thus, the participants' declarations are believed and statistically significant.

The respondents were questioned if glance at a person's biometric information from the database deprived of the owner's consent was a privacy violation. Fifty-four-point-two percent (54.2%) strongly accepted the statement, because the violation of one's private secrecy can result into the individual exposer of a medical record (Singh, 2014). The proposed is to recruit a transparency and honest person running and getting by the biometric system with strict regulations respecting the central and civic liberties. The datum must be utilized solely for the aims quantified. The chi-square value attained is 0.002 and a weighted average of 2.120. Hence, the participants' declarations are statistically substantial.

In advance, participants were quizzed if the biometric data in the database utilized for other reasons than the original purpose was a secrecy violation. Sixty-six-point-one percent (66.1%) strongly accepted and quoted the 2016 incidence in Uganda as the highest surprise, because the voter's biometric thumbprints was retrieved from the NIRA database without owners' consent. The chi-square value attained is 0.000 and a weighted middling of 1.640. Hence, the participants' declaration is considerably. The researcher hence recommends the handlers of the biometric data to be further watchful of users' privacy and individual data distribution. They must visualize that the data is encoded with an authentication key before posting them on the available website. The outcome of the analysis is presented in Table 3.

Table 3**:** The biometric data secrecy

Questionnaires	**SA**	**A**	**N**	**D**	**SD**	**WA**	**χ2 Test**
Non-privacy violation	80.2	19.8	0	0	0	1.20	0.000
New technology abuse	64.8	30.2	0	0	5.2	1.51	0.001
Personal data secrecy	57.8	39.1	0	3.1	0	1.48	0.000
Privacy trespass in database	54.2	19.3	3.4	6.3	16.9	2.12	0.002
Function creep	66.1	24.0	0%	0	9.9	1.64	0.000

SA = Strongly agreed, A = agreed, N = Neutral, D = Disagreed, SD = Strongly disagreed. The t chi-square value beneath 0.050 is significant, the null hypothesis is forbidden while directly overhead 0.050 is not significant, the null suggestion is assumed.

4.5 Factors that influence individuals' distress of the biometric application

This section aimed at understanding the causes of individual fears of the biometric passport application. The analysis concentrated on identifying participants distress of the technology. The 38.8% and 24.2% of the respondents dreaded exposure of individual data, because the biometric data can be utilized for other things than the original planned aim. For example, migration officers at the airfield scan the physical biometric characters of the travelers for recognition against the danger and they necessity a hard drive and internet linking to set out the data, thus odors for other purposes. Forty-eight-point-five percent (48.5%) and 30.5% dreaded inappropriate data transfer, because the exactly file of a person can be exposed against fraud. While the travel archives are kept for comparison purpose, the officer in-charge may use it to trace the records provided for different motives in contrast of the data security requirement. Thus, the information transfer desired to be supervised.

Furthermore, 22.9% and 9.1% presented misuse of biometric data, because the stored data cannot be cancelled once compromised. Suggested is a need for everyone to be more alert on how to protect their identity. It is easy to tell that biometrics are the upcoming security verification, but this forthcoming is undefined except rigorous approaches are used to ensure the protection of the biometric information against any misuse. Eighteen-point-two percent (18.2%) and 7.8% showed unlawful access to private information, because unidentified users can obtain the character authorization to someone else's data and mismanage it, thus deprived of the person consensus. For example, a current situation of Pharmacy2U being penalized a fine of one-hundred-and-thirty-thousand pound (£130 000) by the information manager for

retailing the customers' particulars to 3rd party deprived of consensus (NPA, 2017). This instead brought up the concerns of the user's privacy and numerous dangers in public legislation. The central administration segment, IPP 1, mandate that individual data gathered must be for legal targets. Without awareness and user's concerns, the distress of the biometric application adoption shall remain. Thus, technology developers should look into the consequence of the end-user's worries of the biometric application to draw informed conclusion. The results from the analysis are presented in Fig. 8.

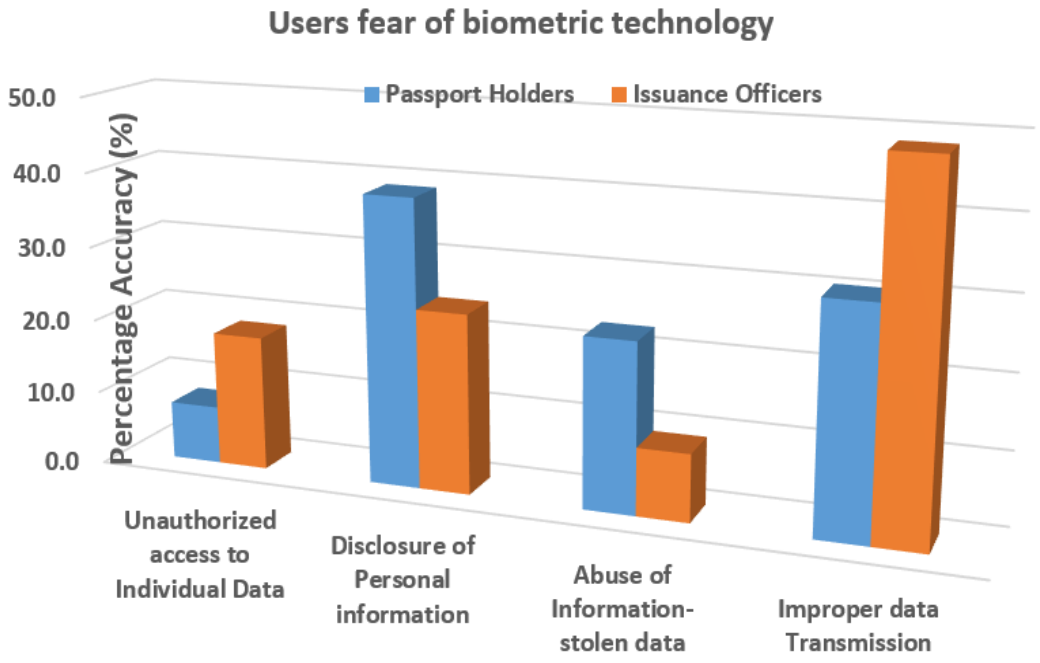


Figure 8**:** Factors influencing users fear of the biometric application

4.6 The security threats of the biometric technology

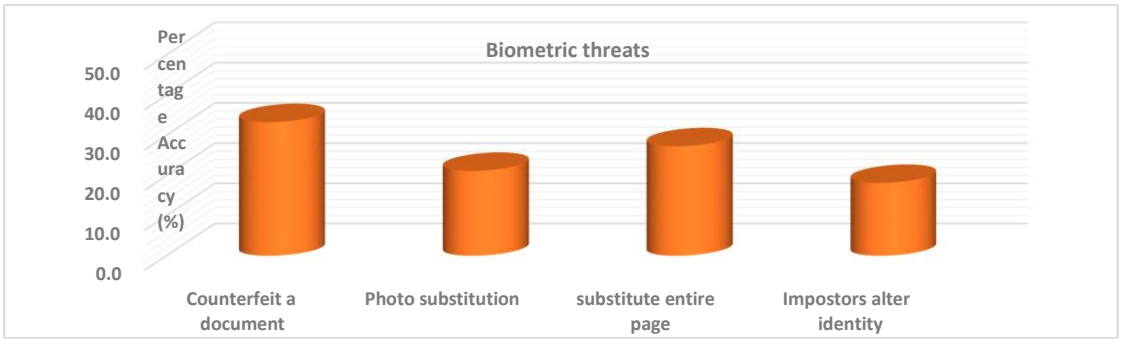
This area of the study explained the important underlying component of the biometric threats experienced. The attacks concerning the biometric data template in the storage database. In the results, 33.3% of the respondents' specified fraud of the biometric data being the highest risk. They indicated that, an impersonator can exchange a fake document to obtain out the illegitimate fraudulent movement. The counterfeit contained illegal reproductions of the original permits unlawfully factory made, either issued or affirmed. Of the several different uniqueness in portable passport documents presented, there is problem to distinguish between false and genuine one. Thus, a need for an INTERPOL to provide numerous dedicated

gadgets for the commandment's passage to notice fake permits and with dissimilar cohorts to amend the degree of safety of authorized permits.

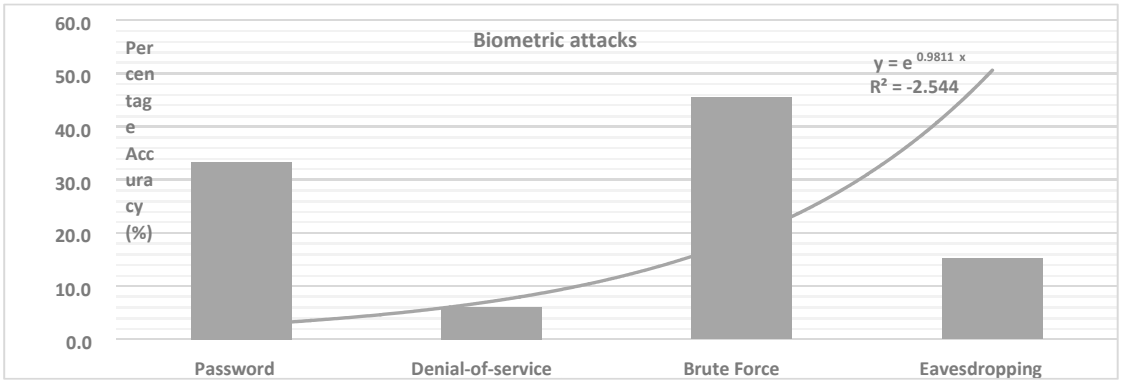
Furthermore, twenty-seven-point-three percent (27.3%) of the respondents indicated the removal and replacement of permit sheets. This is linked with impostors looking forward to alter the genuine permit information sheets of the legitimate holders at the manufacture level. Conventions must be adopted by the community offices to produce harder permits to make it more difficult for the fraudsters to modify or predict.

Additionally, 21.2% showed the threats associated with photo replacement. Photo replacement is eliminating the data picture from the original individuals' permit and modifying it with an impostor's information. Similarly, eighteen-point-two percent (18.2%) presented an impostor's alteration of the identity. The impersonator can amend the biometric traits to adjust the information in a real permit to acquire more confirmation.

Furthermore, the outbreaks to the biometric data template in the storage database are explained. Forty-five-point-five percent (45.5%) of the participants exposed brute-force attack as the risky weakness. While 33.3% presented PIN retrieving, because a masquerader can blow out PIN from the kept application to obtain unlawful records. Also, 15.2% presented eavesdropping. An attacker can secretly spy the communication path and intersects the communication by means of digital devices like the Radio Frequency Identification (RFID) tag. The 6.1% showed Denial-of-service (DoS). Because an invader can try to stop the original operators from retrieving the database application. Hence, 3rd factor authentication is needed to receive PIN secret to avert invaders from compromising specific score. The results of the study are obtainable in Fig. 9a and 9b.



(a)



(b)

Figure 9: (a) The threats of the biometric technology (b) The attack of the biometric technology

Several cases of persons data connected to physical and behavioral characteristics of end-user's acceptance is explained. Fingerprints and facial images received the maximum favorable attention from the participants with forty-four percent (44%) and 32% receptively. This is because fingerprints are used in various national ID systems, institutions and they are more stable. For example, household access control, employees' identification, entrance pass attendance and client recognition. They are simple because the person merely requires to press the sensor interface of the verification device for fingerprint extraction.

Face image is the most acceptable modalities, because people pick out and verify their household, friends and comrades by observing at the expression. Also, 10% of the respondents chosen iris verification, because it is more reliable and secure although tough to operate. The sensory system has been established in various sectors and no record has shown its data breach. The 6% took the signature scan, because they are hard to forge than the regular handwriting. While 4% chose voice scan, 4% chosen Hand scan. The outcomes of the analysis are shown in Fig. 10.

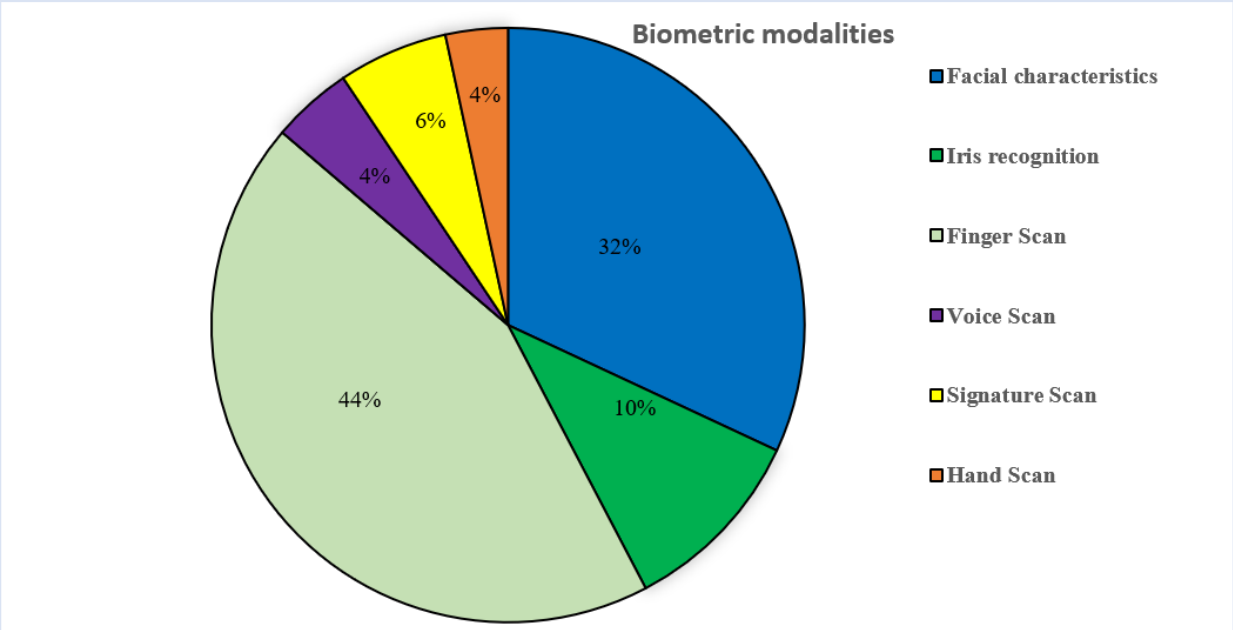


Figure 10: The biometric modalities

The modality limitations associated with acceptance and rejection of the biometric application are explained. For example, the FAR, FRR, Crossover error rate, Received detection traits and the sensor screen. The FRR is the rate of likelihood that the biometric application can incorrectly fail to obtain legal person characteristics. The probability that the biometric application fails to recognize a legitimate user. The formula is given as $FRR = \frac{NFR}{\text{NEVA (NIA)}}$; FRR indicated Failed Reject Rate, NFR is the Non-Failed Rate, the NEVA is the Number of Enrollees Verified Attempt and NIA is the Number of Identified Attempts. However, FAR is the likelihood that the biometric application can incorrectly approve an illegitimate operator. Or possibility that a biometric application can mistakenly identify a personality. The formula is $FAR = \frac{NFA}{\text{NIIA (NIVA)}}$. The FAR is Failed Accept Rate, NFA is Number of Failed Accept, NIIA is Number of Impersonator Identified Attempts and NIVA is Number of Impostors Verified Attempt. The results of the investigation are presented in Table 4.

Table 4: The biometric characteristics

Biometric characters	**Accurateness**	**Simple to use**	**Operator acceptance**	**Speed**	**FAR (%)**	**FRR (%)**
Face image	Medium	High	High	Medium	1%	20%
Iris	High	Medium	Medium	Medium	2%	2%
Fingerprint	High	High	High	High	0.94%	0.99%
Voice	Medium	High	Medium	High	2%	10%
Signature	Medium	Medium	Medium	High	-	-
Hand scan	Medium	High	Medium	High	2%	2%

4.7 Protective measures of the biometric data

Notwithstanding the rise in the outbreaks and intimidations to biometric application, greatest measure to protect and improve the secrecy of the participants data are explained. Sixty percent (60%) and 51.5% of the participants recommended the encryption method and program to secure and protect the biometric data in the database. This is because the encryption protects a classified and sensitive private biometric data and securely stores it in the database.

The 30% of the respondents suggested building data hubs. Because the data hub can offer national resources such as information protection, storage and backup-retrieval. While 58.3% and thirty-three-point-three percent (33.3%) declared identity management, because it helps to scrutinize the organization information, control, manage and guaranteed access to the specific application of the information. The 10% of the respondents suggested the decreased accessibility, because safety is a very vital event in the storage of the administration information. Therefore, the policymakers must consider legalized people in various sectors like public society, industrialization, security experts and government officers. The results of the investigation are shown in Fig. 11a and 11b.

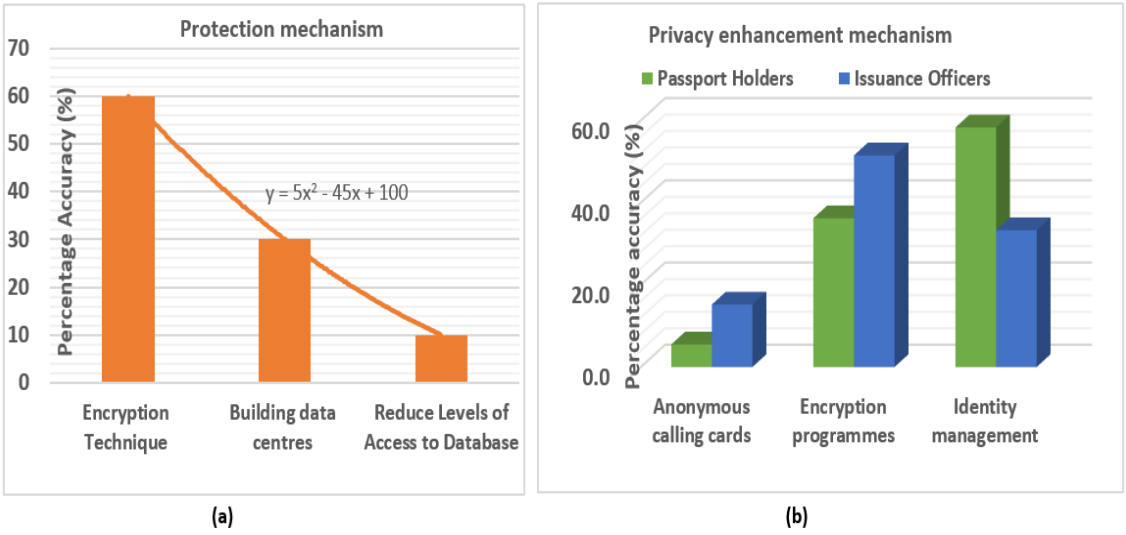


Figure 11: (a) The protection mechanism of the biometric technology, (b) The privacy enhancement of the biometric technology

4.8 The existing biometric passport system

The existing system of the biometric application is based on the information filling and recommendation from the various stake officers. The user either download the form or picks the form from the regional centers to fill. Upon filling, the user attaches the necessary requirement, including payment slip, create a manilla file to save the documents and take them personally to the migration office center within that region. The officer receives the file for verification. If the user does not meet the requirement, the user's file is returned, else the officer verifies the file and delivered them to the headquarter for passport processing. Figure 12 presented the existing framework of the biometric passport system.

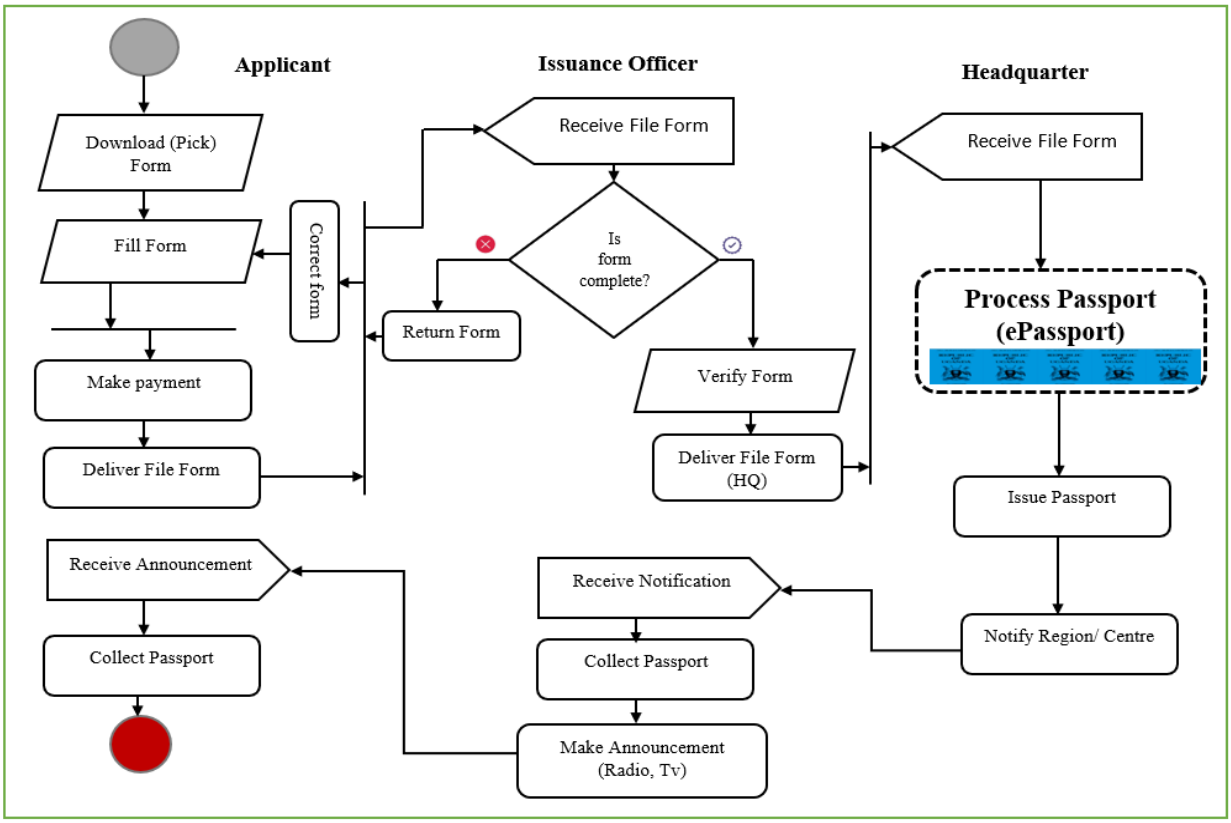


Figure 12: The existing framework of the biometric passport system

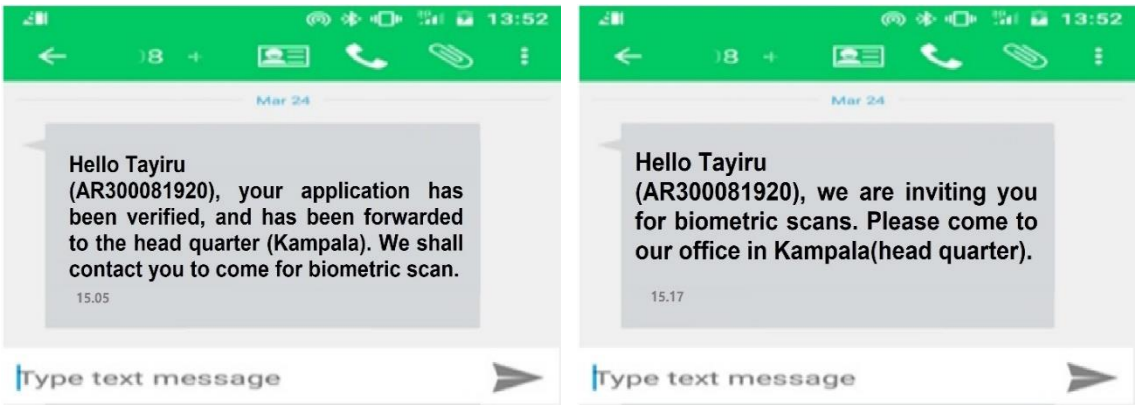
4.9 The proposed system of the biometric application

The proposed system of the biometric application involved five (5) levels. Level 1 input login details to choose the region office. Level 2 and 3 automatic generation of the region code number and form filling. The code number is an exceptional unique number. For example, (AR30081920) code numbers are for the Arua area while (MB66200011920) for Mbale province. This code number defined the region where the user is applying. It defined the area code, month, year and unique applicant number. This helps to trace the route of the applicant and guaranteed the security of the individual information. Level 4 document attachment, like photograph, recommendation letter, coy of NIC and payment slip. Once the passport photo is uploaded, the system automatically encrypts it for security purpose and then decodes it upon the officer's verification.

This facilitate in preventing information linkage and fraudsters from invading on personal data. Level 5 statement declaration and submission. This creates a personnel data access, print a copy before submission to the regional office. Once the officer verified and approved

the application form, the system forwards the details to the headquarter for further processing. Auto-generated SMS message is sent to the user for verification.

The in-charge of headquarter views the candidate's particulars. Once an approval of applicants is performed, the SMS confirmation message for biometric scan is automatically sent to the applicant for the invitation. Figure 13a and 13b illustrated the Twilio SMS send to applicant for verification and biometric scan process.



(a) (b)

Figure 13: (a) Twilio verification message (b) Twilio message for the biometric scan

The biometric traits like the fingerprint, facial image with person's biodata are supplied as an input. The system administrator extracts the fingerprint features (i.e., minutiae points) using the USB suprema BioMini authentication scanner of inbuilt software and the facial image with high definition Logitech pro webcam 1080. The individual presses the fingerprint in the suprema BioMini scanner to interact with the sensing device. The BioStar 2 server is used as an application interface for the biometric feature extraction. BioStar 2 uses several ports to establish device and data communication. The encryption algorithm processes the biometric information to get the encrypted secured data template, then the data is kept in the database. The python flash is used for the development.

Many states are considering biometric technology application submission package with mixture of manual and the automated arrangement to keep biometric data secure. The application alerts any intruder who tries to access person's data. With these security protection mechanisms, researcher is able to tackle users' fears of the individual privacy-protection of the biometric data. Of the worry tackled, access is granted only to those individuals who applied for the application. The persons information is protected and encoded with Twilio SMS message that ensured person's information safety. Each individual

has privileges to access and view the status of the application. Any illegal attempt with individual data, text SMS is automatically sent to the users for the warning, detection and alerting.

The organization is able to manipulate the individual data and provided timely feedback. Therefore, increased correctness and competence. Figure 14 illustrated the suggested architecture of the biometric application system.

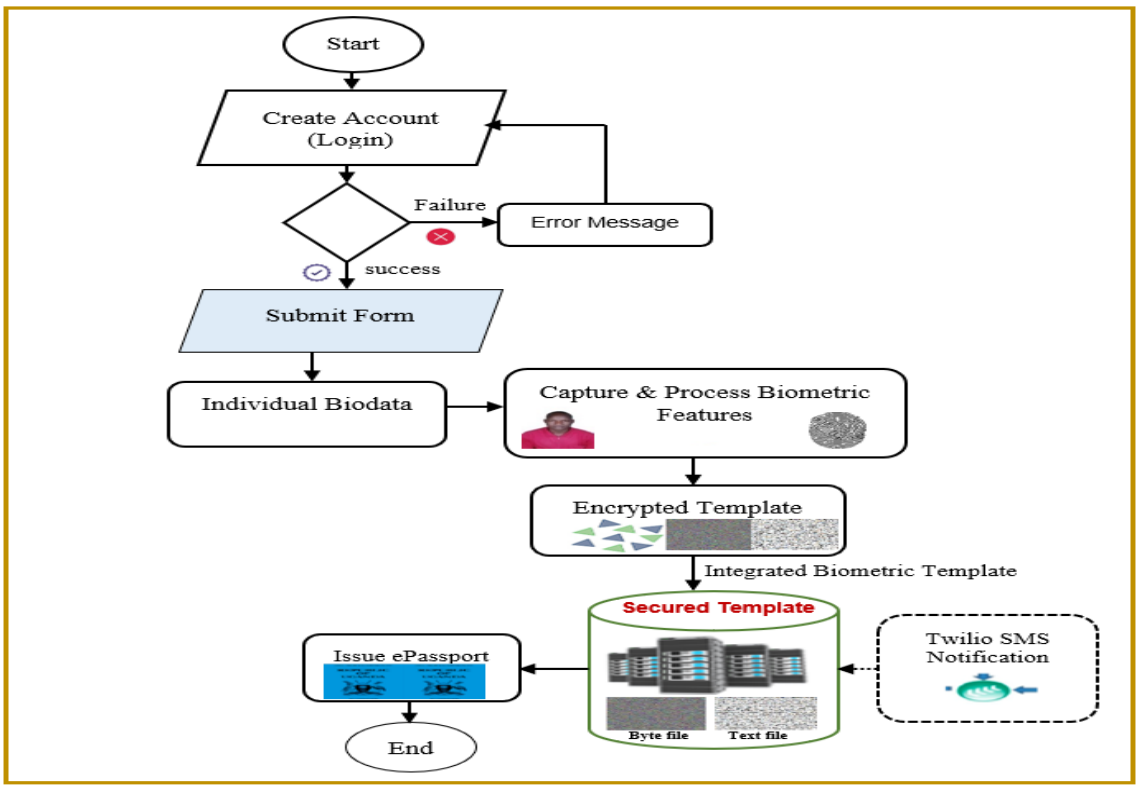


Figure 14: The proposed architecture of the biometric application system

4.10 Security tools used to protect the biometric data template

To enhance the challenges of the stolen biometric data template in the database, data misuse and template modification, different security tools and approach are installed. These tools focused in protecting the biometric data template in the storage database based on the biometric traits such as the fingerprint, facial image with individual's biodata. The security applications installed are Jinja2, Wtforms, SQLAlchemy, Cryptography, Twilio SMS and the encryption-decryption algorithm (Contributors, 2019; Nita, Mihailescu & Pau, 2018).

4.10.1 Jinja2

The Jinja2 is utilized for example, as a template engine. It comprised of the variables and labels to direct the decision. It is a designer-friendly templating language for python, used to secure the optional sandboxed template execution environment. Jinja2 provided a secured outline for mechanization of experiment, trial submission and aids to avoid Cross-Site Scripting (XSS) occurrence through its powerful automatic Hypertext Markup Language (HTML) escaping system. The XSS enabled the invaders to insert customer writings to an internet submission seen from diverse clients. The XSS permits invaders to insert customer-side scripts into homepage observed by other users. The cross-site scripting vulnerability can be used by invaders to bypass access controls.

The primary function of a template engine is to sort out the logic from the horizon. Thus, the template engines considered obeys the following principles:

(i) Restricted set of command structures such as Loop i.e., for loop or while loop, condition i.e., if, elif and else, filter3 i.e., variable filter, setting of variables and printing of a variable.

(ii) Mechanism to include other templates, to use inheritance of templates or to use macros, written entirely in the restricted instructions from above.

(iii) No way to write pure code in the language that is used for the backing (i.e., PHP, Python or Java) within the template.

4.10.2 Wtforms

The Wtforms generates applicant’s passport forms, rather than coding HTML. It secures the application far from Cross-Site-Reference-Forgery (CSRF) unit. The CSRF operation is rotated around the extraordinary token. Note that CSRF is a character of malicious exploitation of a website where unauthorized commands are transported from a user that the web application trusts. Through the Wtforms, the cross-site request forgery attack is prevented.

Notice that, when carrying out the web page form using Wtforms and python, the contours are represented as class representatives. This allowed clearer backend validations before data

proceeds to the database, meaning in case the front-end is tempered with, the Wtforms validations can be capable to manage the authentication.

4.10.3 SQLAlchemy

The SQLAlchemy is used to create the database models. It's one of the most popular and time-tested language for securing the database. It generates storage unit as a replacement for software drivers straightaway. The security gain is to prevent the Structured Query Language (SQL) insertion occurrence, zero-day attack for various databases plus other database exploited through the application. The researcher doesn't code SQL declarations, because a substitute makes the object representative, then SQLAlchemy think out the best and free outbreak SQL declaration correspondence. The SQL expressions can be applied independently of the Object Relational Mapper (ORM). When using the ORM, the SQL expression language remains part of the public face Application Program Interface (API) as it is used within object relational configurations and queries. Notice that SQL injection is the location of malicious code in SQL statements via the web page input (Bayer, 2016). Figure 15 presented a model of SQLAlchemy dependency layers. The SQLAlchemy helped in mapping this class to the corresponding table.

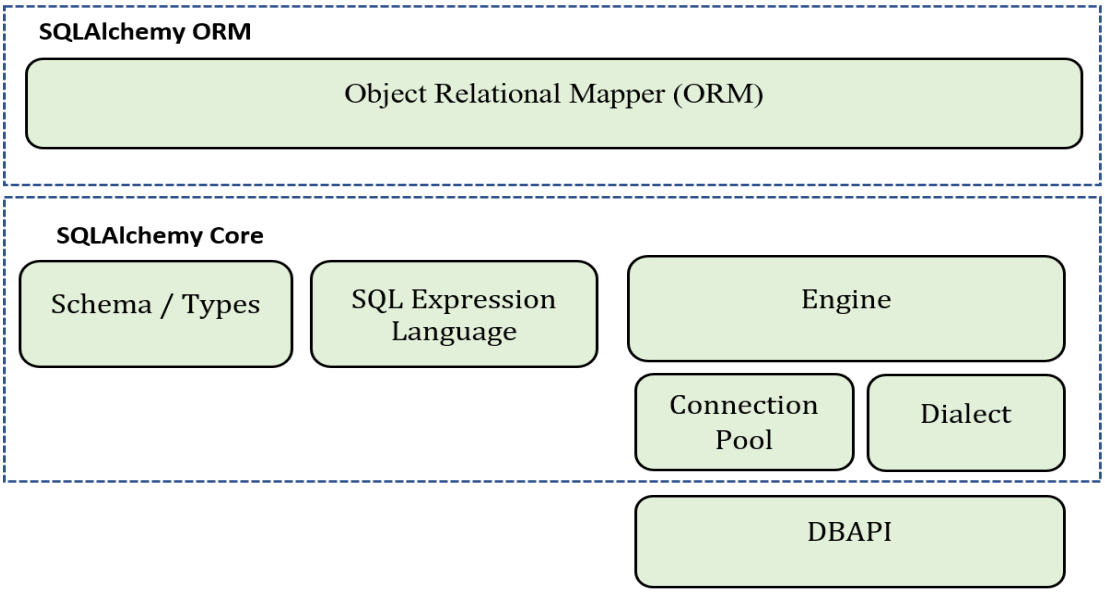


Figure 15: The SQLAlchemy dependencies layers

4.10.4 The cryptography

In cryptography, the plain text is encoded into cipher text with the help of encryption algorithm, the coded text is decoded to plain text with the help of decryption algorithm. In both operations, the cryptographic key played a significant part. It limits the access of the coded data so that the possessor of the key can decrypt cipher text properly. It prevents data from being read by any third party because the system uses a secret key to encrypt and decrypt data which is shared between the sender and receiver. In this technique, it is expected that only the sincere user knows the decryption key. Therefore, cryptography, as a powerful tool in biometric technology, needed an efficient key management technique. The key management technique included the process of key generation, key modification and key sharing (Stallings, 2017).

The cryptography encrypts the fingerprint, facial image using a Fernet keys. The keys are categorized into two smaller keys 128 bits Advanced Encryption Standard (AES) key and a 256 bits Secure Hash Algorithm (SHA) with Hash-Based Message Authentication Code (HMAC) signing key. These keys are retained in a central source that keystone passes in a library to handle the encryption-decryption process. The Fernet keys guaranteed that, the communication encoded cannot be read missing the secret key.

The multiFernet key is generated from the combination of the two Fernet keys to perform the encoded writing using 1st key in the records. Then decodes it one at a time. The key interchange replaced the old key to add a new key Infront. The PIN alternation is accessible by the private key avert damage and decreases the worry of outbreak. Token turning as offered by multiFernet, is the best exercise and the means of cryptographic hygiene, designed to fix damage in case of undetected event and to increase the difficulty of attacks.

4.10.5 The Twilio SMS programmable

The Twilio SMS message is utilized to send users and operators a text message about unlawful entry, in case the officer in-charge is not the one accessing the record. Twilio is a cloud communication system that offers SMS services to its users. It fetches the logs for any outbound messages from the narrative, like the sent folder in the email client. Utilize this data to update the Customer Relationship Management (CRM) whenever a client gets a text message from the application. Or to see the recipients of an SMS message before it sends to ensure they don't receive it before. The Twilio message brings in any inbound messages to

any of the Twilio numbers. This is like the email inbox. If you apply a single Twilio number to commit many types of messages, it can route the responses to the necessary people, founded along the sentiment score of the consistency of the message, who mailed it. Or what time it arrived in. It also sent lots of SMS messages while parabola flow runs. This permits one to send out custom or generic SMS messages to a list of recipients at scheduled times. Use the destination to send the weekly performance, remind occurrence of an event and threats coming up in the system, or constantly ping the user details to remind one of any approval privileges to allow access to the certification.

4.10.6 The suggested MVT-HUF architecture

The suggested operation is called MVT- Helper Utility Filesystem (HUF), an alteration of the Model View Controller (MVC) to secure the biometric data template in the database utilization. The model is a class that manages data rationally. The view indicates the visualization of the datum a model holds. It is employed to execute the business logic and interact with a model to hold data and renders a template. The template contains the data transmission to the model object and keeps view and model differently.

Figure 16a and 16b showed the suggested architecture of the MVT-HUF and the functional intent of the ePassport. The MVT is slightly altered to provide safety measure. For instance, the Wtforms is presented for CSRF security. The helper, presented to hold big processes amongst model and view. The biometric passport is utilized as class represented as a model combining fingerprint and facial image at the character stage with individual's biodata to arise the template files. This template files are steadily kept in the storage incorporated with Twilio SMS. The encryption-decryption algorithm based cryptographic key management is used to ensure the protection of the database template.

The algorithm accounted for the satisfactory inequalities in the biometric involvement. Any impersonator whose trial biometric is different from the enrolled biometric features, cannot break private key. The biometric features encrypted stored an encoded value of the PIN as a template byte and text file. The hashed key can be operated as a cryptographic key, an invader cannot acquire the unique key exterior the encoding scheme.

In Fig. 16b, it's realized that, the encrypted fingerprint and face image is kept in the file system (including the ciphertext of second key). Meanwhile, user biodata is stored in relational tables. It is a significant to recognize that the computer memory in a file system is

implemented using random integers identifications (IDs) that holds less meaning to the user at presentation layers as the presentation level IDs are computed from helpers other than coming from the database.

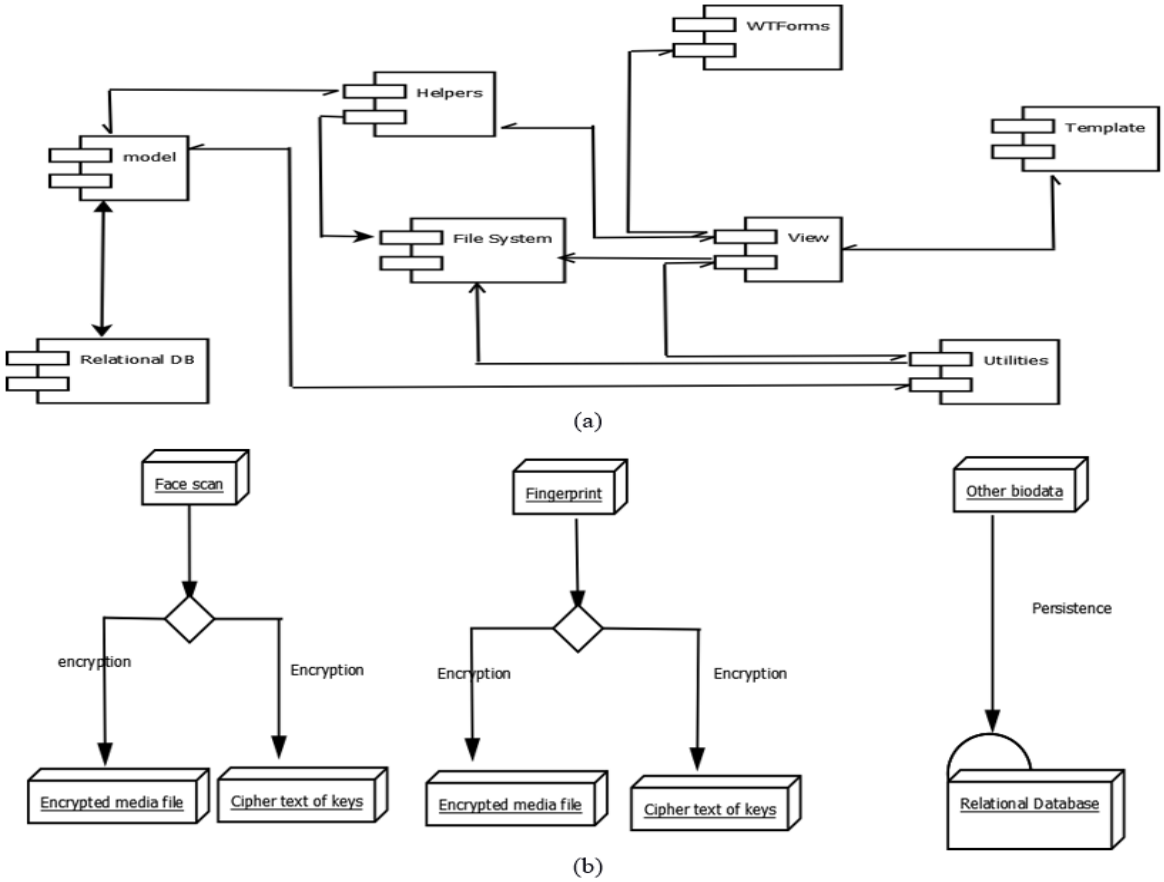


Figure 16: (a) The framework model of the MVT-HUF system, (b) The function design of the ePassport

4.11 The proposed encryption-decryption algorithm and database model

4.11.1 The encryption algorithm

In encryption process, the user input the credentials. The username and password are compared with a copy kept in the database. If the details do not match, the user is requested to re-enter either a new username or password, else if it matches an authentication code is produced and sent to the user via SMS. Upon the user receiving the authentication code, the user is requested to input the received authentication code. The authentication code is matched with a copy that is kept in the database. If the authentication code does not match

with the copy stored in the database, the user is guided back to login interface. If it matches, the database generates two Fernet keys (K_1 and K_2).

The Fernet keys are secret key of symmetric implementation based on cryptography that supports key rotation in the form of byte key. The two keys are combined to further generate multiFernet key (K) for encryption. The K is integrated with biometric features (fingerprint, facial) and biodata passing through the encryption algorithm to produce the biometric data template as byte file and a text file. The two files are incorporated with Twilio SMS message and securely kept in the database as template file. Figure 17 summarized the proposed implementation of the encryption algorithm framework.

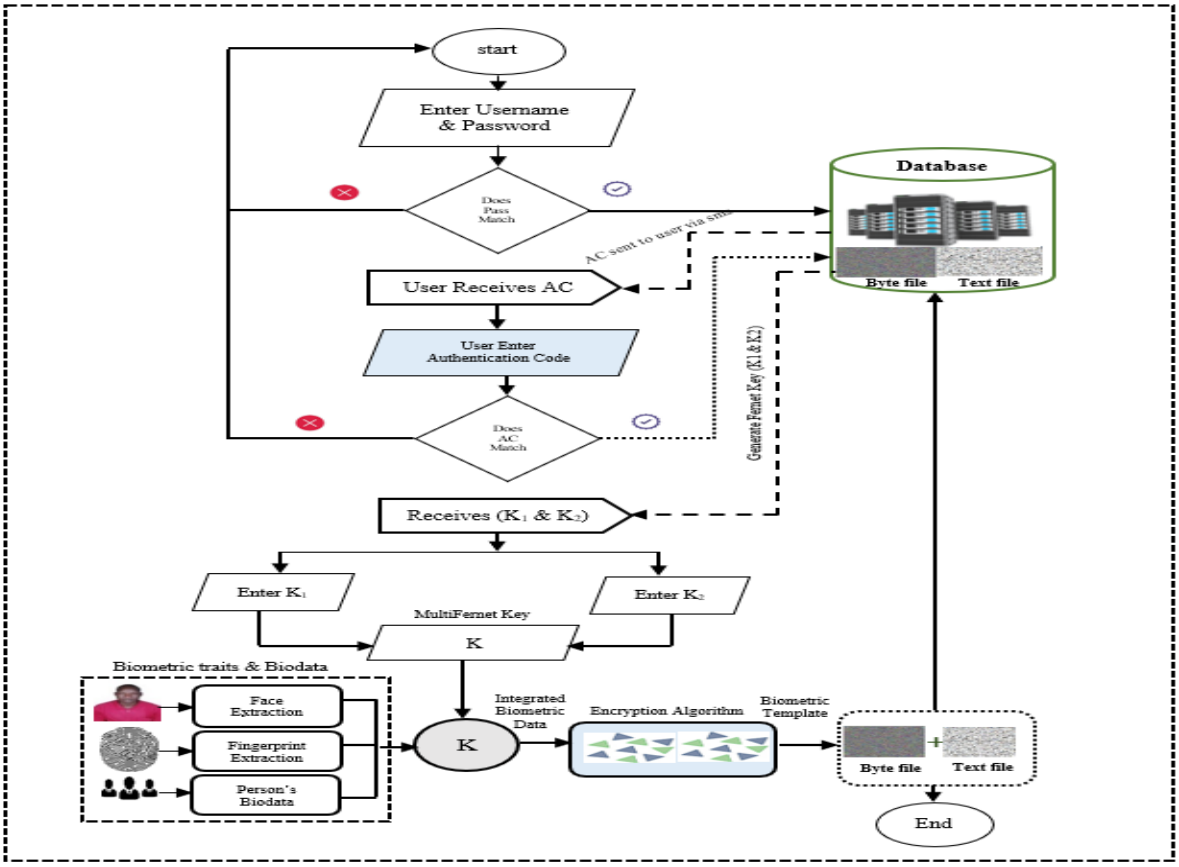


Figure 17: The proposed framework of the encryption algorithm

4.11.2 The decryption algorithm

In decryption process, administrator is required to input the login details. The username and password are compared with a copy that is kept in the database. If the details do not tally, the administrator is requested to re-enter either a new username or password, else if it matches an authentication code is created and sent to the administrator via SMS. Upon receiving the authentication code, the administrator is required to enter the received authentication code. The authentication code that the administrator entered is correlated with a copy that is kept in the database. If the authentication code does not match with the copy stored in the database, the administrator is led back to login interface. If it matches, the database generates the encrypted byte and text files in form of K_{10}. Then administrator enters the two Fernet keys (K_1 and K_2). The two keys are combined to further generate the multiFernet key (K) for decryption. The K is integrated with biometric data template (byte file and text file) passing through the decryption algorithm to produce the plain text. Figure 18 summarized the proposed implementation of the decryption algorithm framework.

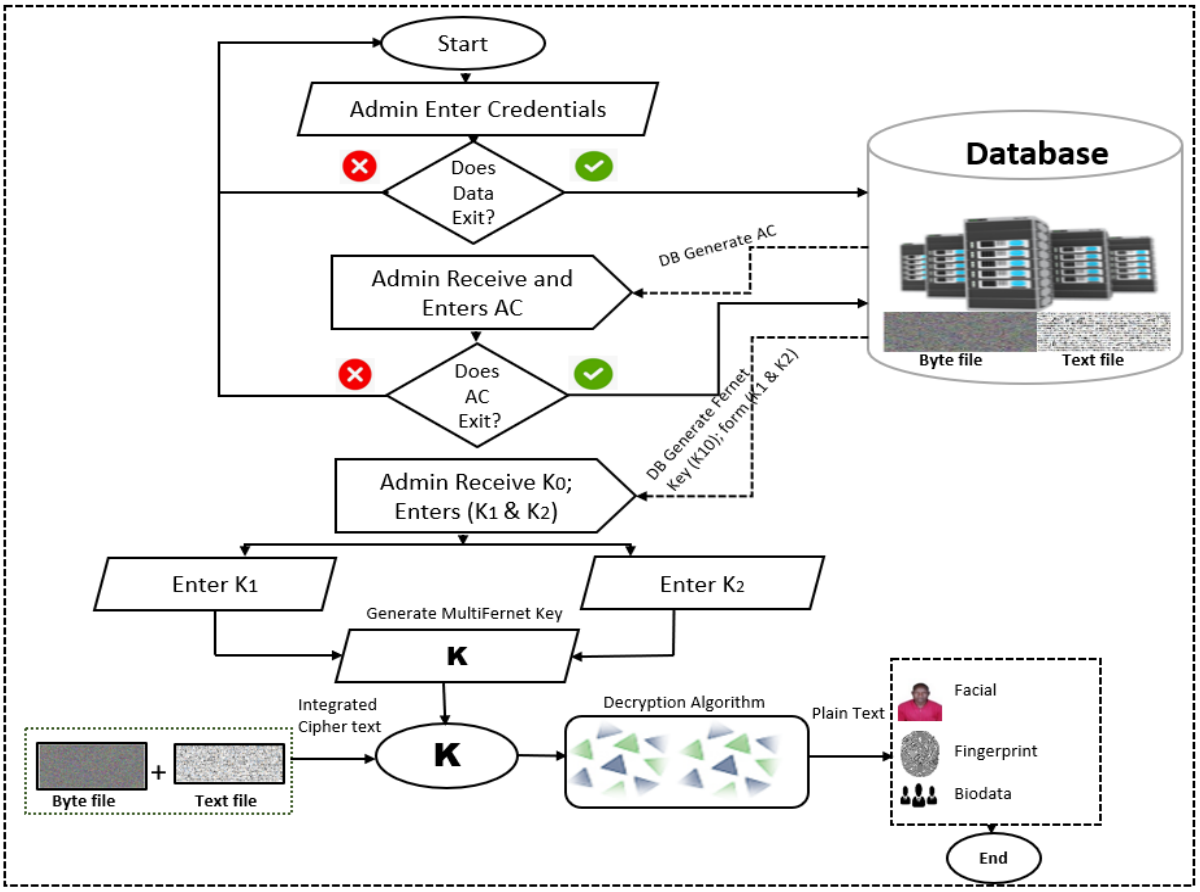


Figure 18: The proposed framework of the decryption algorithm

In the case an attacker attempts to access the biometric data template in the database, the database system will block the attacker from unauthorized access. Because the system cross-verify the attacker based on two different kind of identifications such as the knowledge base (something the user knows) and the possession factor (something the user owns) such as authentication code. This is really important in securing the biometric template information in the database. Even if the perpetrators are able to discover a user's password, they will require the authentication code as second kind of identification needed to login into the application. Figure 19 presented the suggested security measures implemented via the encryption process.

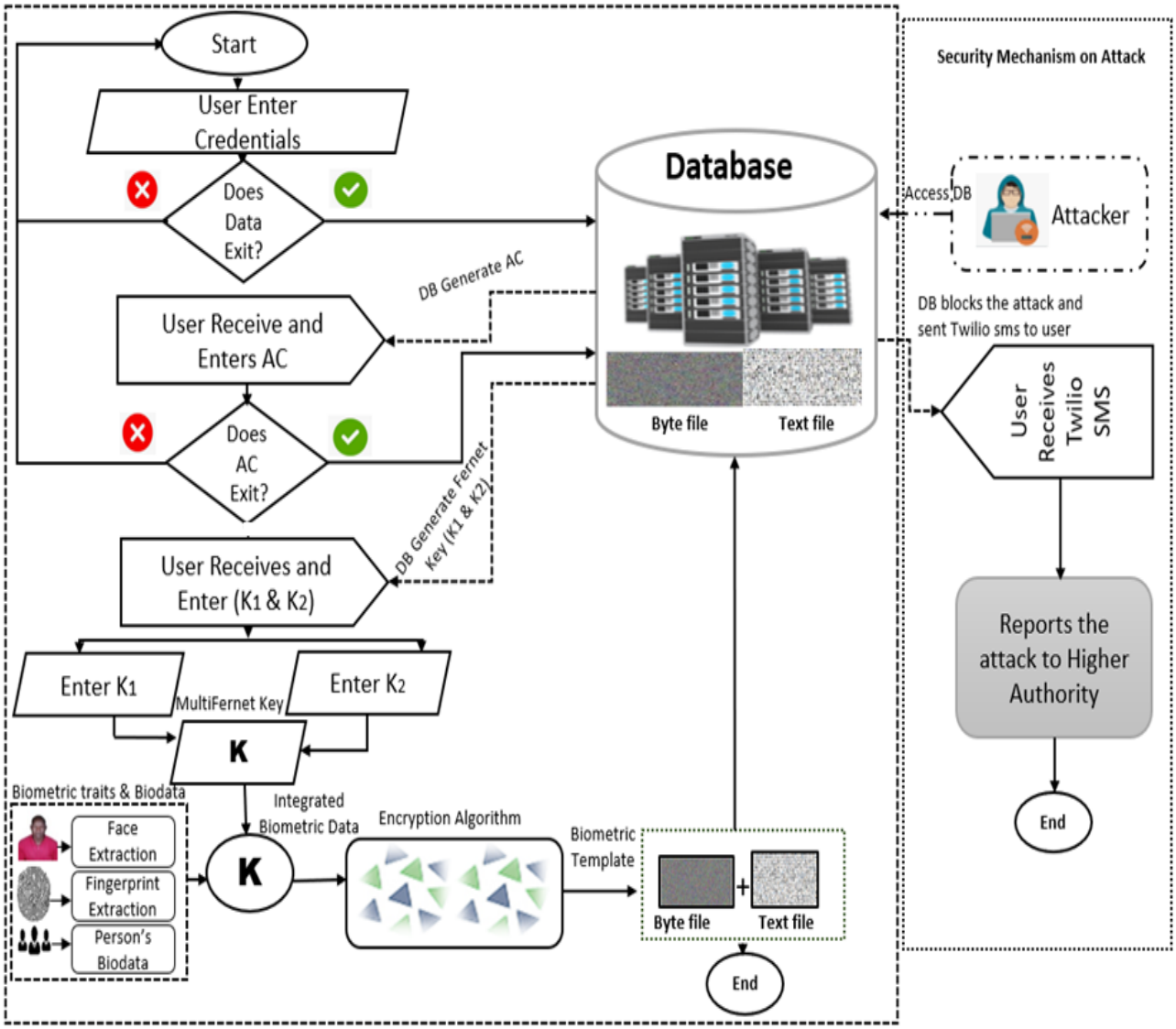


Figure 19: The proposed framework for the security mechanism

4.11.3 Database models

The SQLite3 is used as the proposed model for the development process, and the database switched to PostgreSQL, because of the ORM (SQLAlchemy) for security purpose. It handles a range of workloads, from single machines to data warehouses or Web services with many concurrent users. The PostgreSQL has multi-value fields (a.k.a arrays and nested tables) which can reduce the need for joins. Dramatically increase in the performance of storing and retrieving the multi-dimensional data structures and making it possible to write stored procedures in other programming languages such as C, Perl, Python and JavaScript V8 engine (Bayer, 2016). Figure 20 summarized the database classes of the SQLite3.

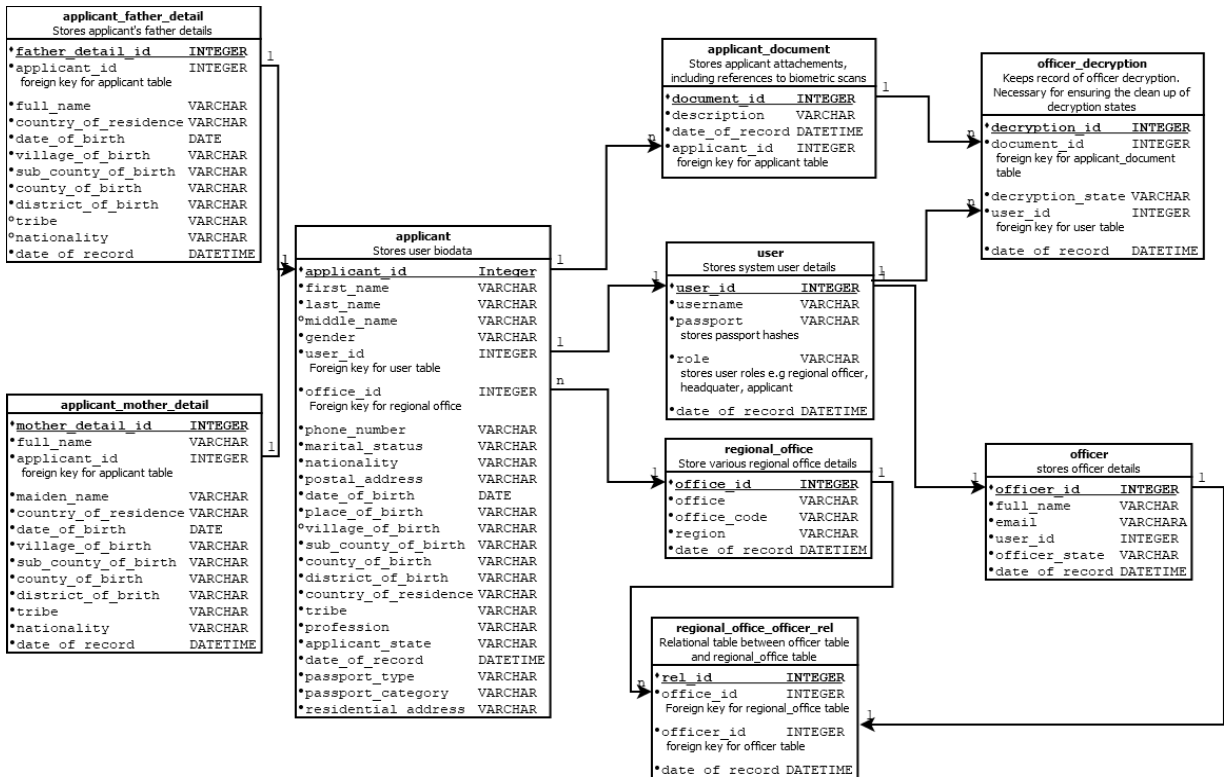


Figure 20: The SQLite3 database classes

4.12 The implementation and evaluation process

The integration of python flask, the sublime as the code editor, Twilio for SMS notification, DB browser SQLite for the database, Biostar 2 server for BioMini suprema and high definition Logitech webcam for biometric feature extraction, win virtual environment and Ubuntu as the testing server with cryptography module are used for the implementation and evaluation process.

4.12.1 The cryptographic of Fernet keys

The cryptographic Fernet keys are built on three criteria. The AES within the Cipher Block Chaining (CBC) mode with a 128-bit keys for encryption using the PKCS7 padding (Fig. 21). The HMAC to secure hashed authentication of two-hundred-fifty-six bits of keys (SHA256). The Initialization Vector (IV) to create a random private code utilizing os.urandom() (Contributors, 2019). AES provides benefits like top-level security and operations doesn't reveal invalid binary.

The AES uses the limits like private key (0,1) either in 128-bits,192-bits or 256-bits lengthy. While CBC uses the padding for block codes. The constraints rest on the IV and private key. The IV is an exceptional public data, arbitrarily changeable at the encoded time to avert data recurrence, ensuring that it's hard for a hacker to get bytes to crack into the template storage. It guaranteed that, data is not trickled by the coded text and disallowed indistinguishable plaintexts from fabricating matching encoded text.

The HMAC is utilized to compute the statement, authentication using cryptographic coded roles, paired off by a private key. This hashed procedure arbitrarily generated the bytes equivalent in duration to the summary size of the private hashed role stored. Figure 21 illustrated the AES block cipher standard.

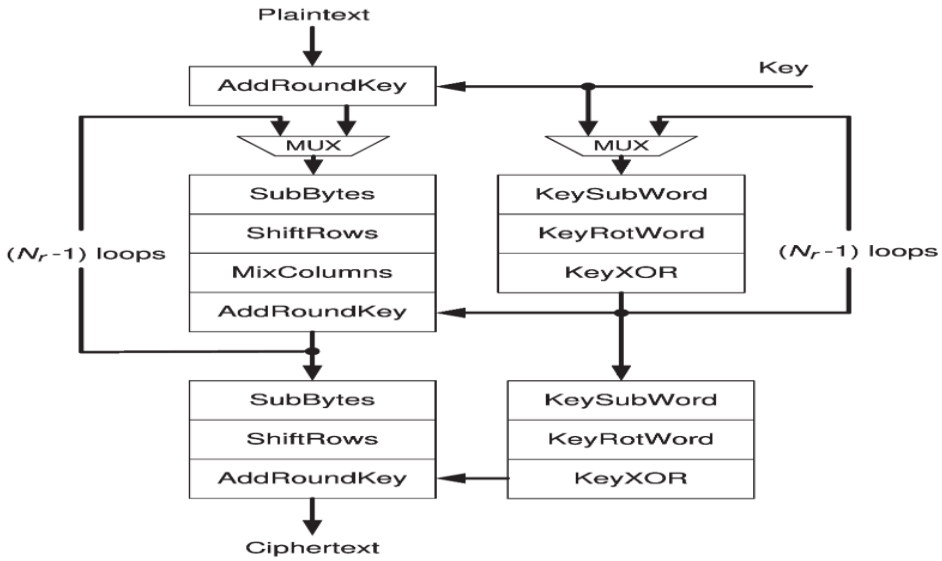
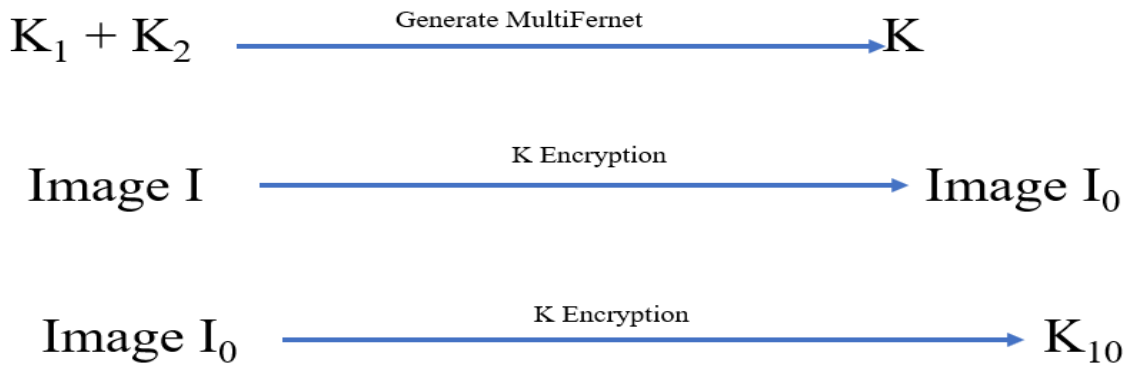


Figure 21: The AES Block (Stallings, 2017)

4.12.2 The key management for the encryption algorithm

The encryption algorithm uses the combination of two Fernet keys, i.e., the initial key (K_1) and the second key (K_2). User inputs original biometric feature Image (I) and K_2 to generate K_1-encoded (byte key). The K_1-encoded is further applied to generate K_1 decoded (string key) using K_2. The K_1 encoded is combined with second key to produce multiFernet key (K). The K is utilized in encrypting image I to realize the encoded image file (I_0). In order to guarantee the safekeeping of the biometric data in the database, the encrypted image (I_0) is further re-encrypted with multiFernet key (K) to produce an encrypted byte and a text file (K_{10}). The two files are incorporated with Twilio sms and securely kept in the database as a template file.

The encryption is the operation of transforming information (plaintext) into something that appears to be random and meaningless (ciphertext) so that it is unclear to anyone but to the intended receiver. Figure 22 summarized the stepwise process for the key management of the encryption algorithm. Presented is the key management using encryption algorithm.



Such that

i. **K1:** First Fernet Key
ii. **K2:** Second Fernet Key
iii. **K:** multiFernet key
iv. **Image I:** Original face scan image or fingerprint Image
v. **Image Io:** Encrypted biometric image
vi. **K10:** Encrypted byte file and text file

Figure 22: The key management of the encryption algorithm

4.12.3 The multiFernet encryption algorithm

The multiFernet is generated from fernet suite that consists of various block ciphers as illustrated in Fig. 23.

MultiFernet Encryption Algorithm

Input: Image bytes, password P

Key Generation: kdf= {Ko, K1)
Kdf=PBKDF2(P, SHA256, HMAC256)
Such that:
PBKDF2=Password-based key derivation Function 2;
SHA256= 256 bits Secure Hash Algorithms
HMAC256=256 bits Hash-based Message Authentication Code

Generate cipher suite: C128
C128=AES10(kdf, I)
Such that:
AES10= 128 bits Advanced Encryption Standard

Generate timestamp: TS64
Such that:
TS64= 64 bits

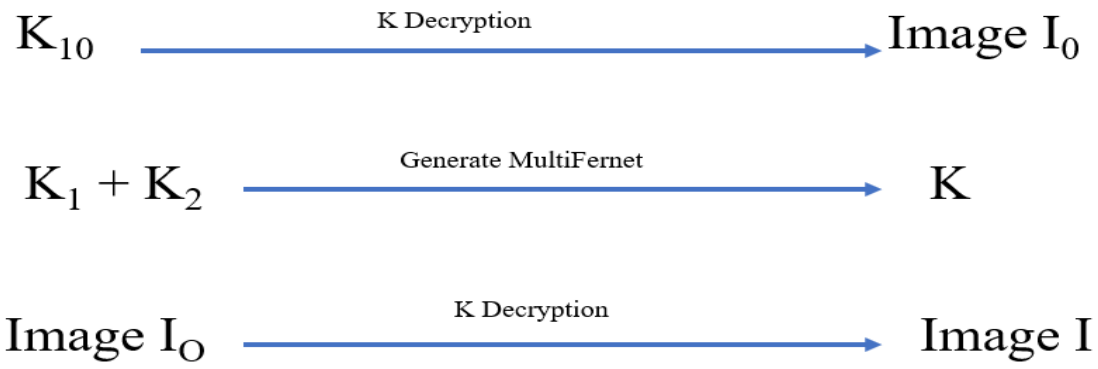
Generate Block Cipher: B0
Such that:
B0=Concant (V8, TS64, IV126, C128)
V8= version 8 of fernet
IV126= 126 bits Initial Vector

Figure 23: The multiFernet key implementation

4.12.4 The key management for the decryption algorithm

To obtain the unique image (I) from the encoded byte and text file (K_{10}), the decryption procedure is reversed engineering of the encoded step. The K_{10} is decrypted using the multiFernet key (K) to realize the encrypted Image I_0. The K is generated from the combination of K_1 and K_2. The K is further employed to decrypt the encrypted image I_0 to yield the original image I. When formatted token is positively decoded, the unique plain text image (I) is acknowledged as the result, else exception error is produced.

The decryption operates by changing encrypted information (secret code text) back to readable plaintext so that it is understandable again. Figure 24 summarized the stepwise process for the key management of the decryption algorithm. Given below is the stepwise procedures for the key management.



Such that

i. **K_{10}:** Encrypted byte file and text file
ii. **K_1:** First Fernet Key
iii. **K_2:** Second Fernet Key
iv. **K:** multiFernet key
v. **Image Io:** Encrypted biometric image
vi. **Image I:** Original face image or fingerprint Image

Figure 24: The key management of the decryption algorithm

4.12.5 The performance evaluation of the algorithm

The performance evaluation of the algorithm is based on how accurate a biometric system is, i.e., measure of its performance by applying a varying score threshold to the similarity scores (Biometrics, 2014). The results can either be presented as a pair, i.e., FRR at a certain level of FAR, or in plots (Fig. 2). The rates can be expressed in many ways, for instance, in percent (1%), decimal format (0.010) or by using powers of ten (10^2).

Some systems don't inform a similarity score, only the match/nonmatch decision. In that case it is only possible to gain a single FRR/FAR pair (and not a continuous series) as result of a performance evaluation. If the mode of operation (the security level) is adjustable (i.e., it can have a means of controlling the internally used score threshold), else the performance evaluation can be run again and again in different modes to obtain further FRR/FAR pairs.

There are basically three categories of performance evaluations i.e., technology, scenario and operational evaluation. In technology evaluation, the evaluation uses the saved data, for instance, previously acquired fingerprint images. In scenario evaluation, the evaluation uses end-to-end system prototype or simulated environment. In operational evaluation, the evaluation uses the performance of a complete biometric system to determine the specific application environment with a specific population.

The technology evaluations are by far the most common and often feasible. Because the evaluation is done using saved samples, and the outcomes are reproducible and it is less time consuming. The greatest disadvantage is that they do not necessarily reflect the conditions where the system will eventually be used. Because of this, it can be beneficial to collect a dedicated set of samples trying to mimic the conditions of the target system when preparing for an evaluation.

Going back to the prototype of the developed system, the performance evaluation of the algorithm was based on the inputs from the users. Three factors were considered for the evaluation process:

(i) Performance, is the system accurate to achieve the intended purpose.
(ii) Acceptability, are users willing to accept the system in their daily lives.
(iii) Convenience, is the system easy to use by users and difficult to hack by an attacker.

A total sample of 150 respondents from three universities were registered in the prototype system. Sixty-six percent (66%) of the respondents expressed positive willingness in using the system. The 40% cited ease to use, 28.67% specified security privileges and 31.33% expressed convenience. These henceforth, informed the investigator that the stored biometric data template provided the level of security needed on the user's biometric data template in the database.

4.13 Discussion of the results

This study is conducted with the purpose of identifying and analyzing users' fears of biometric technology and to build up an efficient algorithm for securing the biometric data template in the database. To accomplish this purpose, the study tried to achieve this aim by fulfilling the four specific objectives shown in section 1.4.2. It is essential to determine the

vulnerabilities and attacks against biometric technology from the existing literature and finding ways to protect and secure the biometric data template in the database.

The study, therefore, attempts to resolve the subsequent research questions such as: How secure is biometric technology used in the biometric passport acquisition? How people's biometric data are being held within the passport attainment? What potential privacy-security dangers and users' fears are related to biometric technologies? What countermeasure do users recommend to protect the biometric data template in the database?

4.13.1 How secure is biometric technology used in the biometric passport acquisition?

A substantial effect to investigate the safety of biometric technology is identified based on the wider knowledge of the biometric passport acquisition by the respondents. The answers indicated that 69.3% agreed that the biometric technology is more dependable than the tradition-based protection method. Because it plays a big part in controlling security of information within an organization. While 30.7% disagreed, quoting that the biometric technology can be violated and abused by an impostor. Thus, a requirement for person's mindfulness about the safety and privacy of the data distribution in the everyday various registration events (Fig. 6).

4.13.2 How people's biometric data are being handled during the passport issuance?

This question proved to investigate the fundamental factors of users feeling towards the biometric information handling. It focused the analysis to identify if the participants studied, had worries of the technology (Fig. 8). Thirty-eight-point-three percent (38.8%) and 24.2% of the respondents dreaded exposure of individual data. This is because the biometric data can be utilized for other things than the original planned aim. Forty-eight-point-five percent (48.5%) and thirty-point-five percent (30.5%) are afraid of improper data transfer, because the document of the person can be exposed to fraud. Because the records may be tracked, the files may be given in response to a data security requirement. Hence, the information transfer requires careful monitoring and a tracking device. Additionally, 22.9% and nine-point-one percent (9.1%) presented misuse of information. Because the DNA information can expose a person's health disease.

So, mindfulness and user's fears need to be addressed, because the fear of the adoption of the biometric technology still remain a question to answer. This study, therefore, can aid the

technology creators to realize the important insight of the user's worries on the acceptance of the biometric application and helps draw a better conclusion.

4.13.3 What is the potential privacy-security risks and users' fears regarding the biometric technologies?

This question tried to explain the fundamental threats experienced in the issuing of the biometric passport in relation to users' fears. The probe of the factors prompting participants fear in using the biometric technology as well as the safekeeping with the suggested solutions for the implementation of the biometric application. The results obtained in the aforementioned (Fig. 8) showed that the common worries are related to exposer of personal data, the abuse of personal information and unauthorized access. It can be concluded that, forged travel document is the highest encountered security risk. Because the identity scam of travel documents is the broad range of crimes and terrorism committed globally Fig. 9a and 9b. The same conclusion can be drawn that individual data collected need to be collected for legitimate purpose. Accordingly, guidelines need to be adhered by the public citizens to ensure that the passport documents are standard and harder for the impostors to forge and predict and easy for the authority to trace where, when, how and by whom the identity fraud.

In light of the above threats related to biometric technology, users fear that some wrongdoers around the workplaces and illegal contractors of the association can possibly abuse the personal information for another intended purpose. The suggested is an appropriate policy maker to craft policies that warns in contrast to data linkages of individual information. Because information is resided wherever in the online and can be stolen by fraudsters in the present information systems.

4.13.4 What countermeasure do users recommend to protect the biometric data template in the database?

This question proved to serve the third objective that required getting an algorithm to enhance the privacy and safety template of the biometric application. Users expressed encryption technique as the greatest measures to protect and improve the privacy of the user's data Fig. 11a and 11b. The encryption technique helps protect the biometric sensitive private data and enhance the security of the database communication. The encryption algorithm is based on the cryptographic module of Fernet keys instance, where two Fernet keys are combined to generate a multiFernet key (K) for the encryption. The two (2) unreadable encrypted byte file

and text file is created. These files are incorporated with Twilio message and securely stored in the database server. Thus, prevented data being compromised by an impostor. Living by the framework in (Fig. 17), the same conclusion can be drawn near the model. It can be well-known that no biometric application is ideal. The determination as to which biometric is to be used can be prepared by the foundation of the operation and the kind of application as well as the degree of protection required.

The Twilio SMS is implemented for the validation over unlawful access to application template. For an attacker attempting to access data template in the database, the system blocks the attacker from unauthorized access. Because the system can cross-verify the attacker based on something it owns such as authentication code. The Twilio SMS message fetch the login for any outbound messages from the application as well as any inbound messages to any of the Twilio numbers.

The Linux 18.040 is utilized as a customer storage to offer an interaction and allowed individual call for resources. The users and the server each have separate jobs to accomplish. Figure 25 summarized the customer-storage structure.

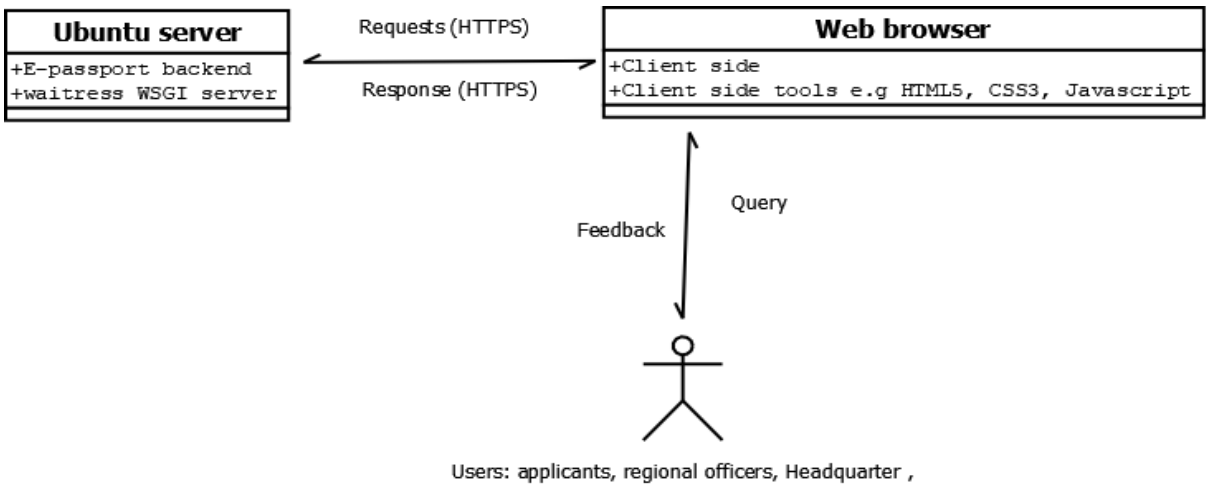


Figure 25: The client-server architecture

The results are verified with user's biometric traits, containing fifty (50) fingerprints and fifty (50) facial image templates incorporated with the personal biodata. The 256 X 256 resolution is used. The facial image is uniformly illuminated and taken from the right mind with no tilting and with a plain background color. The end product of the image is set to 600dpi with 120 pixels as the standard, recommended by ISO/IEC (Griffin & Ph, 2005; Tistarelli &

Nixon, 2009). The BioStar 2 server was used as the platform interface for the biometric feature extraction. The encrypted byte and text files are incorporated with Twilio programmable SMS. The Twilio SMS message is auto-generated directly from the database to alert users in circumstance an attacker attempted to access the database. The text message is one of the security mechanisms successfully implemented. It helped inform the users and the officer the protected data template in the storage database and how individuals are indirectly involved in awarding or refusing access to the exercise of the biometric template information.

The analysis outcomes of the study are explained based on the users concerns and knowledge of biometric passport technology. The proposed framework of the encryption-decryption algorithm on the cryptographic component using multiFernet key instance are explained in details. User data template in the database is securely protected. The findings of the proposed approach outweigh the previous studies in a way that, the proposed approach provided high level of security that guard against impostor's attack, because access to user's biometric data in the database is controlled and monitored. The privacy and security risks of the biometric data as well as unauthorized access to database server is secured. Because the database server can block the attacker from unauthorized access, cross-verify the attacker based on the possesses, such as authentication code and finally sent Twilio SMS message to user for confirmation. This study therefore, surpass the previous studies that looked at the identification of attacks at the biometric template database, security and accuracy mechanism to biometric template protection based on transformation as well as privacy weakness of the biometric template using the biometric sketches.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The aim of the study is to develop an algorithm to improve the secrecy and security template of biometric technology. As biometric technology applied to many applications, the study focused within the biometric passport. The survey received two major objective functions, the analysis factors to user's concerns and knowledge as well as the algorithm to improve the secrecy and security template of the biometric technology. The objectives are to identify users' concerns and fears relating to the biometric passport technology and to develop an effective algorithm to secure the biometric data template in the database.

The methodology deployed are based on survey study and encryption-decryption algorithm method. Three-hundred-and-eighty-four (n=384) participants are documented holders, while thirty-three (n=33) respondents are issuance officers. The analysis results indicated that users have secrecy and security fears like an exposer of individual information, inappropriate data transfer, misuse of individual information as well as forging document and brute-force attack.

The encryption-decryption algorithm method is developed to encode the biometric data in the database. The encoded data produced two encrypted template files (byte and text files). The two enciphered byte and text files are incorporated with Twilio message and securely kept in the database server. The storage has security measures that guarded in contrast to impostors' outbreak together with persons data. Any potential compromise of the user's data within the center area or regional offices is recognized. The access to the database system is controlled and monitored. The biometric data offered high level of security to the users' data privacy and integrity. In circumstances where an attacker attempts to access the biometric data template in the database, the system blocks the attacker from unauthorized access and cross-verify the attacker based on the validation of its ownership i.e., authentication code. Even if the perpetrators are able to discover a user's password, they will lack the second kind of identification required to log into the application.

This study, therefore, contributed to the awareness of the users' fears of privacy and security issues, especially on biometric passport acquisition. Because non-technological topics like factors promoting the adoption of the technology and individuals expected worries are

explained in details. Second, the development of the secured algorithm for protecting the biometric data template in the database based on the multiFernet key generated from the Fernet keys instance. The multiFernet key limits the damage in the event of an undetected event and to increase the difficulty of brute-force attacks. For instance, if a worker who had access to the organization Fernet key leaves, you can generate new Fernet key, rotate all of the tokens currently deployed using that new key, and then retire the old Fernet key(s) to which the employee had access. Third, the implementation of Twilio SMS message in alerting the users and the officers in the case any attacker tries to hack the database server. Fourth the scientific publication to the body of knowledge as well as the prototype of ePassport system that enable users to apply online.

Lastly, the study can inspire practitioners of the technology to carefully weigh the likely benefits and thoroughly assess the hazards connected with the implementation of this technology in a broader logic before engaging themselves in full production. In conclusion, the biometric technology should be developed from the foundation of the operation of the application and the degree of protection required.

5.2 Recommendations

The following are the recommendations portrayed from the research results presented:

(i) The policymaker to design security policies to protect against the vulnerabilities of users' biometric information. Because individual's data exist in everyplace online and security concerns are particularly salient on the use of the biometric data.

(ii) A prerequisite to facilitate the database server with additional safety coding like hash functions and two factor authentications to prohibit data requests transmission. Setting out principles and alertness session to all mediators at the start of the engagement before being granted access to personal information.

(iii) The industrial creator to propose a passport permit that is really hard to create. Centralize database centre appropriately to safeguards the data template and allows the public adoption of the biometric application with self-enrollment.

(iv) Audit all the system verification and identification activities needed at the database level to determine all successful and failed attempts for analysis and scrutiny by

biometric system designers. This will significantly detect anomalies and identify threats of present biometric technology.

(v) The databases of biometric systems where biometric data templates are stored should have the access points controlled by using biometrics in preference to use of traditional authentication modes like passwords so that only authorized and trusted users e.g., biometric system designer are able to manage these databases and this will in addition, prevent hacking of database passwords.

Other results achieved in this thesis, raised further interesting and challenging questions. Thus, a need for upcoming research pertinent to employ satisfactions of user's willingness and adoption of the biometric technology without compromising their privacy and security. The submissions for upcoming study are:

(i) Further study, utilizing the multi-biometric and multi-factor authentication systems, focusing upon the iris and the retina for high security application and performance.

(ii) Research on ways to derive encryption keys from either fingerprint, face or iris that do not change with repeated scans and makes it difficult for the brute-force attack.

(iii) Future work to develop a mobile application for the biometric technology (ePassport). Capable of helping the immigration authorities to discover fraud and extract records from stored fraudster. The mobile application should automatically place the position of someone accessing the persons' information and register it to the organization.

REFERENCES

Ailisto, H., Lindholm, M., Mäkelä, S. M., & Vildjiounaite, E. (2004). Unobtrusive user identification with light biometrics. *In Proceedings of the third Nordic Conference on Human-Computer Interaction*, 327–330.

Akhtar, Z., Micheloni, C., & Foresti, G. L. (2015). Biometric liveness detection: Issue and research opportunities. *IEEE Security & Privacy*, 13(5), 63–72.

Al-Saggaf, A. A., & Acharya, H. (2013). Statistical Hiding of the Fuzzy Commitment pattern for Securing Biometric Templates. *International Journal of Computer Network and Information Security*, 5(4), 8.

Alaswad, A. O. (2014). Vulnerabilities of Biometric Authentication "Threats and Countermeasures". *International Journal of Information and Computation Technology*, 4(10), 947–958.

Alshar'e, M., Zin, A. M., Sulaiman, R., & Mokhtar, M. R. (2015). Evaluation of the TPM user authentication model for trusted computers. *Journal of Theoretical and Applied Information Technology*, 81(2).

AlTarawneh, M. S., Woo, W. L., & Dlay, S. S. (2008). Fuzzy vault crypto biometric key based on fingerprint vector features. *In 2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, 452–456.

Ambalakat, P. (2005). Security of biometric authentication systems. *In 21st Computer Science Seminar*, 1.

Ang, R., Safavi-Naini, R., & McAven, L. (2005). Cancelable key-based fingerprint templates. *In Australasian Conference on Information Security and Privacy*, 242–252.

Anitha, P., Rao, K. N., Rajasekhar, V., & Krishna, C. H. (2017). Security for Biometrics Protection between Watermarking and Visual Cryptography. *SSRG International Journal of Electronics and Communication Engineering*, 64–71.

Ao, S., Ren, W., & Tang, S. (2008). Analysis and reflection on the security of biometrics system. *In 2008 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 1–5.

Arjunwadkar, M., Kulkarni, R. V., & Shahu, C. (2012). Biometric Device Assistant Tool: Intelligent Agent for Intrusion Detection at Biometric Device using JESS. *International Journal of Computer Science Issues*, 9(6), 366–370.

Armoogum, S., & Oozeer, A. R. (2016). A practical approach for secure biometric template storage for authentication. *In 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies*, 71–175.

Ashish, M. M., & Sinha, G. R. (2016). Biometric Template Protection. *Journal of Biostatistics and Biometric Application*, 1(2), 1-7.

Ashok, J., & Shivashankar, V. (2006). An overview of biometrics. *Journal of Acta Technical Napocensis*, 2(7), 2402–2408.

Avoine, G., Kalach, K., & Quisquater, J. J. (2008). ePassport: Securing international contacts with contactless chips. *In International Conference on Financial Cryptography and Data Security*, 141–155.

Awad, A. I., & Hassanien, A. E. (2014). Impact of Some Biometric Modalities. In Computational Intelligence in Digital Forensics: *Journal of Forensic Investigation and Applications*, 47–62

Bayer, M. (2016). SQLAlchemy Documentation. SQLAlchemy Documentation Release 0.7.10. Retrieved from papers3: //publication /uuid/ 5E97B936-E845-4995-92F5-EB7F0C39672B

Berg, B. L. S. U. (2008). *Qualitative Research Methods for the Social Sciences.* (S. Kelbaugh & K. Hanson, Eds.) (4th ed.). Boston: Pearson Education.

Billeb, S., Rathgeb, C., Reininger, H., Kasper, K., & Busch, C. (2015). Biometric template protection for speaker recognition based on universal background models. *Journal of IET Biometrics*, 4(2), 116–126.

Biometrics, P. (2014). White-Paper, Understanding biometric performance evaluation. *AB–SPA*, 133(1000), 4160

Böhm, C., Färber, I., Fries, S., Korte, U., Merkle, J., Oswald, A., & Wackersreuther, P. (2011). Efficient database techniques for identification with fuzzy vault templates. *In BIOSIG*, 115-126

Bolle, R. M., Connell, J. H., & Ratha, N. K. (2002). Biometric perils and patches. *Pattern Recognition Journal*, 35(12), 2727–2738.

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27–40.

Brindha, V. E., & Natarajan, A. M. (2012). Multi-modal biometric template security: Fingerprint and palmprint based fuzzy vault. *Journal of Biometrics and Biostatistics*, 3(3), 100–150.

Busch, C. (2012). ISO / IEC Standard 24745 - Biometric Information Protection.

Cappelli, R., Ferrara, M., & Maltoni, D. (2010). Minutia cylinder-code: A new representation and matching technique for fingerprint recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(12), 2128–2141.

Chaudhary, S. (2013). An Approach to Secure Database Templates in Multi modal Biometric Systems. *International Journal of Computing Science and Communication*, 4(2), 268–273.

Christian, R., & Christoph, B. (2012). Multi-Biometric Template Protection: Issues and Challenges. *New Trends and Developments in Biometrics, 173-190*

Coli, P., Marcialis, G. L., & Roli, F. (2008). Fingerprint silicon replicas: static and dynamic features for vitality detection using an optical capture device. *International Journal of Image and Graphics*, 1–19.

Contributors, I. (2019). Cryptography Documentation.

Dodis, Y., Reyzin, L., & Smith, A. (2004). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *In International Conference on the Theory and Applications of Cryptographic Techniques*, 523–540.

Draper, S. C., Khisti, A., Martinian, E., Vetro, A., & Yedidia, J. S. (2007). Using distributed source coding to secure fingerprint biometrics. *In Acoustics, Speech and Signal Processing, IEEE International Conference*, 2(1), 129

Du, E. Y., Yang, K., & Zhou, Z. (2011). Key incorporation scheme for cancelable biometrics. *Journal of Information Security*, 2(4), 185.

Dürmuth, M., Oswald, D., & Pastewka, N. (2016). Side-Channel Attacks on Fingerprint Matching Algorithms. *In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*, 3–13.

Dwivedi, R., & Dey, S. (2019). A novel hybrid score level and decision level fusion scheme for cancelable multi-biometric verification. *Journal of Applied Intelligence*, 49(3), 1016–1035.

El-Abed, M., Lacharme, P., & Rosenberger, C. (2012). Security evabio: An analysis tool for the security evaluation of biometric authentication systems. *In 2012 5th IAPR International Conference on Biometrics*, 460–465.

Elkamchouchi, H. M., Shawky, M. A., Takieldeen, A. E., Fouda, I. M., Khalil, M. M., Elkomy, A. A., & AbdElrasol, A. K. (2018). A new image encryption algorithm combining the meaning of location with output feedback mode. *In 2018 10th International Conference on Communication Software and Networks*, 521-525.

Emmanuel, E., Edebatu, D., Catherine, N., & Ngozi, A. (2016). Vulnerability of Biometric Authentication System. *International Journal of Innovative Research in Science, Engineering and Technology*, 2742–2749.

Gaddam, S. V. K., & Lal, M. (2010). Efficient Cancelable Biometric Key Generation Scheme for Cryptography. *International Journal of Network Security*, 11(2), 61–69.

Galbally, J., Cappelli, R., Lumini, A., Gonzalez-de-Rivera, G., Maltoni, D., Fierrez, J., & Maio, D. (2010). An evaluation of direct attacks using fake fingers generated from ISO templates. *Journal of Pattern Recognition Letters*, 31(8), 725–732.

Galbally, J., Cappelli, R., Lumini, A., Maltoni, D., & Fierrez, J. (2008). Fake fingertip generation from a minutiae template. *In 2008 19th International Conference on Pattern Recognition*, 1–4.

Geethanjali, N., Thamaraiselvi, K., & Priyadharshini, R. (2012). Feature level fusion of multibiometric cryptosystem in distributed system. *International Journal of Modern Engineering Research*, 2(6), 4643–4647.

Geetika, M. K. (2013). Fuzzy Vault with Iris and Retina: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(4).

Ghouzali, S., Lafkih, M., Abdul, W., Mikram, M., El-Haziti, M., & Aboutajdine, D. (2016). Trace attack against biometric mobile applications. *Journal of Mobile Information Systems*, 2016.

Gobi, M., & Kannan, D. (2014). A Secured Public Key Cryptosystem for Biometric Encryption. *International Journal of Computer Science and Information Technologies***,** 5(1), 184–191.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, 8(4), 597–607.

Gomez-Barrero, M., Maiorana, E., Galbally, J., Campisi, P., & Fierrez, J. (2017). Multi-biometric template protection based on homomorphic encryption. *Journal of Pattern Recognition*, 67, 149–163.

Griffin, P., & Ph, D. (2005). Understanding the Face Image Format Standards.

Habibu, T., & Sam, A. E. (2018). Assessment of vulnerabilities of the biometric template protection mechanism. *International Journal of Advanced Technology and Engineering Exploration*, 5(45), 243–254.

Hadid, A., Evans, N., Marcel, S., & Fierrez, J. (2015). Biometrics systems under spoofing attack: an evaluation methodology and lessons learned. *IEEE Signal Processing Magazine,* 32(5), 20–30.

Hooda, R., & Gupta, S. (2013). Fingerprint Fuzzy Vault: A Review. *International Journal*, 3(4), 479-482.

Imamverdiyev, Y., Teoh, A. B. J., & Kim, J. (2013). Biometric cryptosystem based on discretized fingerprint texture descriptors. *Journal of Expert Systems with Applications,* 40(5), 1888–1901.

Jacobsen, E. K. U. (2012). Unique Identification: Inclusion and surveillance in the Indian biometric assemblage. *Journal of Security Dialogue,* 43(5), 457–474.

Jain, A. K., Flynn, P., & Ross, A. A. (2007). Handbook of biometrics. *Springer Science and Business Media.*

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008, 1-17.

Jain, A. K., Nandakumar, K., & Nagar, A. (2013). Fingerprint template protection: From theory to practice. *In Security and Privacy in biometrics*, 187–214.

Jain, A. K., Pankanti, S., Prabhakar, S., Hong, L., Ross, A., & Wayman, J. L. (2004). Biometrics: A Grand Challenge. In ICPR (2) (pp. 935–942). *In Proceedings of the 17th International Conference on Pattern Recognition*, 2, 935-942.

Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE Transactions on Information Forensics and Security,* 1(2), 125–143.

Jain, A. K., Ross, A., & Uludag, U. (2005). Biometric template security: Challenges and solutions. *In Signal Processing Conference, 2005 13th European*, 1–4.

Jeng, A. B., & Chen, L. Y. (2009). How to enhance the security of e-passport. *In Machine Learning and Cybernetics, 2009 International Conference on IEEE, 5, 2922–2926.*

Jeny, J. V., & Jangid, C. J. (2013). Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion. *International Journal of Emerging Technology and Advanced Engineering*, 3(3).

Jin, A. T. B., Ling, D. N. C., & Goh, A. (2004). Biohashing: two factor authentication featuring fingerprint data and tokenized random number. *Journal of Pattern Recognition*, 37(11), 2245–2255.

Joshi, M., Mazumdar, B., & Dey, S. (2018). Security Vulnerabilities Against Fingerprint Biometric System. *Journal of Information Security*, 1–27.

Juels, A., & Sudan, M. (2002). A Fuzzy Vault Scheme Proc. *In Intl Symp. Inf. Theory, A Lapidoth, E. Teletar*, 408.

Juels, A., & Wattenberg, M. (1999). A fuzzy commitment schemes. *In Proceedings of the 6th ACM Conference on Computer and Communications Security*, 28–36.

Kalvet, T., Karlzén, H., Hunstad, A., & Tiits, M. (2018). Live Enrolment for Identity Documents in Europe. *In International Conference on Electronic Government, Springer*, 29–39.

Kamaldeep, K. (2011). A Review of Various Attacks on Biometrics System and Their Known Solutions. *International Journal of Computer Technology and Applications*, 2(6).

Kang, H., Lee, B., Kim, H., Shin, D., & Kim, J. (2003). A study on performance evaluation of the liveness detection for various fingerprint sensor modules. *In International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, Springer*, 1245–1253.

Khan, S. H., Akbar, M. A., Shahzad, F., Farooq, M., & Khan, Z. (2015). Secure biometric template generation for multi-factor authentication. *Journal of Pattern Recognition*, 48(2), 458–472.

Kholmatov, A., & Yanikoglu, B. (2006). Biometric cryptosystem using online signatures. *In International Symposium on Computer and Information Sciences*, Springer, 981–990.

Kim, W. (2017). Fingerprint liveness detection using local coherence patterns. *IEEE Signal Processing Letters*, 24(1), 51–55.

Krause, M. (2001). The expanding surveillance state: why Colorado should scrap the plan to map every driver's face and should ban facial recognition in public places. *Independence Institute, Issue Paper*, 8, 2001.

Kumar, V. K. N., & Srinivasan, B. (2013). Internet Passport Authentication System Using Multiple Biometric Identification Technology. *International Journal of Information Technology and Computer Science*, 5(3), 79–89.

Latha, U., & Rameshkumar, K. (2013). A Study on Attacks and Security Against Fingerprint Template Database. *International Journal of Emerging Trends and Technology in Computer* Science, 2(5).

Lee, C., Choi, J. Y., Toh, K. A., Lee, S., & Kim, J. (2007). Alignment-free cancelable fingerprint templates based on local minutiae information. *IEEE Transactions on Systems, Man, and Cybernetics*, 37(4), 980–992.

Li, P., Yang, X., Cao, K., Tao, X., Wang, R., & Tian, J. (2010). An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications*, 33(3), 207–220.

Li, S., & Kot, A. C. (2011). Privacy protection of fingerprint database. *IEEE Signal Processing Letters*, 18(2), 115–118.

Liu, E., & Zhao, Q. (2017). Encrypted domain matching of fingerprint minutia cylinder-code (MCC) with l1minimization. *Journal of Neurocomputing*, 259, 3-13.

Liu, L., Li, Y., Cao, Z., & Chen, Z. (2017). One Private Broadcast Encryption Scheme Revisited. *International Journal of Electronics and Information Engineering*, 7(2), 88–95.

Maio, D., Maltoni, D., Capelli, R., Franco, A., Ferrara, M., & Turroni, F. (2013). FVC-onGoing: on-line evaluation of fingerprint recognition algorithms. URL https: //Biolab. Csr. Unibo. It/Fvcongoing/UI/Form/Home. Aspx.

Malhotra, S., & Kant, C. (2013). A Novel approach for securing biometric template. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(5).

Maniroja, M., & Sawarkar, S. (2013). Biometric Database Protection using Public Key Cryptography. *International Journal of Computer Science and Network Security*, 13(5), 20–28.

Manvjeet, K., & Sanjeev, S. D. S. (2010). Template and Database Security in Biometrics Systems: A Challenging Task. *International Journal of Computer Applications*, 4(5), 2–6.

Marasco, E., & Ross, A. (2015). A survey on antispoofing schemes for fingerprint recognition systems. *Journal of ACM Computing Surveys*, 47(2), 28.

Marcel, S., Nixon, M. S., & Li, S. Z. (2014). Handbook of biometric anti-spoofing, *Springer*, 1.

Matsumoto, T., Matsumoto, H., Yamada, K., & Hoshino, S. (2002). Impact of artificial "gummy" fingers on fingerprint systems. In Optical Security and Counterfeit Deterrence Techniques. *Journal of International Society for Optics and Photonics*, 4677(4), 275–289.

Meenakshi, V. S., & Padmavathi, G. (2010). Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault. *International Journal of Computer Science Issues*, 7(5), 159.

Minakshi, G., RupKumar, D., Deepjyoti, M., & Rupam, D. M. B. (2012). A Secured Template Based Face Recognition Technique. *Journal of Computer Science and Information Technology*, 75–93.

Ministry of East African Community Affairs in conjunction with the Directorate of Citizenship and Immigration Control, M. of I. A. (2012). East African Community. Report.

Mm, A., & Gr, S. (2017). Biometric Template Protection. *Journal of Biostatistics and Biometric Applications*, 1(2), 1–8.

Moon, D., Choi, W. Y., Moon, K., & Chung, Y. (2009). Fuzzy fingerprint vault using multiple polynomials. *In 2009 IEEE 13th International Symposium on Consumer Electronics*, 290–293.

Mordini, E. (2008). Biometrics, human body, and medicine: A controversial history. *In Ethical, Legal and Social Issues in Medical Informatics on IGI Global*, 249–272.

Mwema, J., Kimani, S., & Kimwele, M. (2015). A Study of Approaches and Measures aimed at Securing Biometric Fingerprint Templates in Verification and Identification Systems. *International Journal of Computer Applications Technology and Research,* 4(2).

Mwema, J., Kimwele, M., & Kimani, S. (2015). A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates. *International Journal of Computer Trends and Technology,* 20(1), 12–18.

Nagar, A., Nandakumar, K., & Jain, A. K. (2010). Biometric template transformation: a security analysis. In Media Forensics and Security. *Journal of International Society for Optics and Photonics,* 7541(2), 75410

Nagar, A., Nandakumar, K., & Jain, A. K. (2012). Multibiometric cryptosystems based on feature-level fusion. *IEEE Transactions on Information Forensics and Security*, 7(1), 255–268.

Nandakumar, K., & Jain, A. K. (2008). Multibiometric template security using fuzzy vault. *In 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*, 1-6.

Nandakumar, K., & Jain, A. K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine, 32(5)*, 88–100.

Nandakumar, K., Jain, A. K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing*, 2008, 1-17.

NIRA-Uganda. (2015). Mass registration of pupils and students.

Nita, S. L., Mihailescu, M. I., & Pau, V. C. (2018). Security and cryptographic challenges for authentication based on biometrics data. *Journal of Cryptography*, 2(4), 39.

NPA. (2017). Pharmacy2U is NOT your local pharmacy and has nothing to do with us.

O'Leary, Z. (2004). The Essential Guide to Doing Research (First). London: *SAGE Publications Ltd.*

Pagnin, E., & Mitrokotsa, A. (2017). Privacy-Preserving Biometric Authentication: Challenges and Directions. *Journal of Security and Communication Networks,* 2017, 1–9.

Panigrahy, S. K., Jena, D., Korra, S. B., & Jena, S. K. (2009). On the privacy protection of biometric traits: palmprint, face, and signature. *In International Conference on Contemporary Computing, Springer*, 182–193.

Patel, V. M., Ratha, N. K., & Chellappa, R. (2015). Cancelable biometrics: A review. *IEEE Signal Processing Magazine,* 32(5), 54–65.

Phillips, P. J., Scruggs, W. T., O'Toole, A. J., Flynn, P. J., Bowyer, K. W., Schott, C. L., & Sharpe, M. (2007). FRVT 2006 and ICE 2006 large-scale results. *National Institute of Standards and Technology*, 7408(1).

Poongodi, P., & Betty, P. (2014). A Study on Biometric Template Protection Techniques. *International Journal of Engineering Trends and Technology*, 7(4).

Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: security and privacy concerns. *IEEE Security and Privacy Magazine,* 1(2), 33–42.

Pratiba, D., & Shobha, G. (2013). A Novel approach for securing biometric template. *International Journal of Advanced Research in Computer Science and Software Engineering*, 3(6), 974–979.

Przybocki, M., & Martin, A. F. (2004). NIST speaker recognition evaluation chronicles. *In ODYSSEY04-The Speaker and Language Recognition Workshop*, (2), 12-22.

Radha, N., & Karthikeyan, S. (2010). A study on biometric template security. *ICTACT Journal of Soft Computing*, 1(2010), 37-41.

Raju, S. V., Vidyasree, P., & Madhavi, G. (2014). Enhancing Security of Stored Biometric Template in Cloud Computing Using FEC. *International Journal of Advanced Computational Engineering and Networking,* 2(2), 35–39.

Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M. (2007). Generating cancelable fingerprint templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence,* 29(4), 561–572.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An analysis of minutiae matching strength. *In International Conference on Audio-and Video-Based Biometric Person Authentication, Springer,* 223–228.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal,* 40(3), 614-634.

Rathgeb, C., Gomez-Barrero, M., Busch, C., Galbally, J., & Fierrez, J. (2015). Towards cancelable multi-biometrics based on bloom filters: A case study on feature level fusion of face and iris. *In Biometrics and Forensics, 2015 International Workshop on IEEE,* 1–6.

Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security,* 2011, 1–22.

Riaz, N., Riaz, A., & Khan, S. A. (2018). Biometric template security: An overview. *Journal of Sensor Review*, 38(1), 120–127.

Rindai, V. C. (2016). Biometric voter registration: Lessons from Ugandan polls.

Roberts, C. (2007). Biometric attack vectors and defences. *Journal of Computers and Security,* 26(1), 14–25.

Rosenberger, C. (2018). Evaluation of Biometric Template Protection Schemes based on a Transformation. *International Conference on Information System Security and Privacy*, 216–224.

Ross, A. A., Shah, J., & Jain, A. K. (2005). Toward reconstructing fingerprints from minutiae points. In Biometric Technology for Human Identification. *Journal of International Society for Optics and Photonics, 5779(2),* 68–80.

Ross, A., Nandakumar, K., & Jain, A. K. (2008). Introduction to multibiometric. *In Handbook of biometrics on Springer*, 271–292.

Ross, A., Shah, J., & Jain, A. K. (2007). From template to image: Reconstructing fingerprints from minutiae points. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(4), 544–560.

Sandhya, M., Prasad, M. V. N. K., & Chillarige, R. R. (2016). Generating cancellable fingerprint templates based on Delaunay triangle feature set construction. *Journal of IET Biometrics*, 5(2), 131–139.

Schmitt, V., & Jordaan, J. (2013). Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. *International Journal of Computer Applications*, 68(23).

Schuckers, S. A. C. (2002). Spoofing and Anti-Spoofing Measures. *Information Security Technical Report*, 7(4), 56-62.

Shalabh, K. (2014). Chapter 4 Stratified Sampling. Retrieved from http://home.iitk.ac.in /~shalab/sampling/chapter4-sampling-stratified-sampling.pdf

Shelton, J., Bryant, K., Abrams, S., Small, L., Adams, J., Leflore, D., & Dozier, G. (2012). Genetic and evolutionary biometric security: Disposable feature extractors for mitigating biometric replay attacks. *Procedia Computer Science Journal*, 8, 351–360.

Simoens, K., Bringer, J., Chabanne, H., & Seys, S. (2012). A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Transactions on Information Forensics and Security*, 7(2), 833-841.

Singh, S. C. (2014). Confidentiality and Disclosure in the Practice of Medicine and Healthcare Services. *Institute of Development Management*, 1(3), 313.

Sontowski, S. (2018). Speed, timing and duration: contested temporalities, techno-political controversies and the emergence of the EU's smart border. *Journal of Ethnic and Migration Studies*, 44(16), 2730–2746.

Stake, R. E. (2010). Qualitative Research: Studying How Things Works. *Journal of Chemical Information and Modeling*, 53(1).

Stallings, W. (2017). Cryptography and network security: *Principles and Practice.* Pearson Upper Saddle River.

Storisteanu, D. M. L., Norman, T. L., Grigore, A., & Labrique, A. B. (2016). Can biometrics beat the developing world's challenges? *Journal of Biometric Technology Today,* 2016(11), 5-9.

Supriya, V. G., & Manjunatha, S. R. (2014). Chaos based Cancellable Biometric Template Protection Scheme a Proposal. *International Journal of Engineering Science Invention,* 3(11), 14–24.

Tams, B. (2013). Attacks and countermeasures in fingerprint based biometric cryptosystems. *ArXiv Preprint ArXiv*, 1304-7386.

Tan, B., & Schuckers, S. (2006). Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. *In 2006 Conference on Computer Vision and Pattern Recognition Workshop on IEEE,* 26.

Teoh, A. B. J., & Kim, J. (2007). Secure biometric template protection in fuzzy commitment scheme. *Journal of IEICE Electronics Express,* 4(23), 724–730.

Tigga, R., & Wanjari, A. (2013). Survey on Template Protection Scheme for Multimodal Biometric System. *International Journal of Science and Research*, 4(7), 768-772.

Tistarelli, M., & Nixon, M. S. (2009). Advances in Biometrics: *Third International Conferences, ICB 2009, Alghero, Italy on Springer,* 5558.

Topcu, B., Erdogan, H., Karabat, C., & Yanikoglu, B. (2013). Biohashing with fingerprint spectral minutiae. *In 2013 International Conference of the BIOSIG Special Interest Group on IEEE,* 1–12.

Topcu, B., Karabat, C., Azadmanesh, M., & Erdogan, H. (2016). Practical security and privacy attacks against biometric hashing using sparse recovery. *EURASIP Journal on Advances in Signal Processing*, 1–20.

Uludag, U., & Jain, A. K. (2004). Attacks on biometric systems: A case study in fingerprints. In Security, Steganography, and Watermarking of Multimedia Contents. *Journal of International Society for Optics and Photonics*, 5306, 622–633.

Uludag, U., Pankanti, S., & Jain, A. K. (2005). Fuzzy vault for fingerprints. *In International Conference on Audio-and Video-Based Biometric Person Authentication on Springer*, 310–319.

Vakalis, I. (2011). Privacy and biometric passports. *The Scientific World Journal*, 11, 478–489.

Wilson, C., Hicklin, A. R., Bone, M., Korves, H., Grother, P., Ulery, B., & Watson, C. (2004). Fingerprint vendor technology evaluation 2003: Summary of results and analysis report. *NIST Technical Report NISTIR*, 7123.

Xi, K., & Hu, J. (2010). *Bio-Cryptography*. Handbook of Information and Communication Security, 129–157.

Yang, H., Jiang, X., & Kot, A. C. (2009). Generating secure cancelable fingerprint templates using local and global features. *In 2009 2nd IEEE International Conference on Computer Science and Information Technology*, 645–649.

Yang, W., Hu, J., Fernandes, C., Sivaraman, V., & Wu, Q. (2016). Vulnerability analysis of iPhone 6. *In 2016 14th Annual Conference on Privacy, Security and Trust on IEEE*, 457–463.

Yang, W., Hu, J., Wang, S., & Wu, Q. (2018). Biometrics based privacy-preserving authentication and mobile template protection. *Journal of Wireless Communications and Mobile Computing*, 2018.

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. *Journal of Symmetry*, 11(2), 141.

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2018). A fingerprint and finger-vein based cancelable multi-biometric system. *Journal of Pattern Recognition*, 78, 242–251.

Yoon, S., Feng, J., & Jain, A. K. (2012). Altered fingerprints: Analysis and detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 34(3), 451–464

Zhang, P., Hu, J., Li, C., Bennamoun, M., & Bhagavatula, V. (2011). A pitfall in fingerprint bio-cryptographic key generation. *Journal of Computers & Security*, 30(5), 311–319.

Zheng, G., Fang, G., Shankaran, R., & Orgun, M. A. (2015). Encryption for implantable medical devices using modified one-time pads. *IEEE Access Journal*, 3, 825–836.

Zheng, G., Fang, G., Shankaran, R., Orgun, M. A., Zhou, J., Qiao, L., & Saleem, K. (2017). Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. *IEEE Journal of Biomedical and Health Informatics*, 21(3), 655–663.

Zheng, G., Shankaran, R., Orgun, M. A., Qiao, L., & Saleem, K. (2017). Ideas and challenges for securing wireless implantable medical devices: A review. *IEEE Sensors Journal*, 17(3), 562–576.

APPENDICES

Appendix 1: Qualitative questionnaire for passport issuance officers

Implemented by

Nelson Mandela African Institution of Science and Technology (NM-AIST)
School of Computational and Communication Science and Engineering

Consent Statement

I am a staff of Muni University currently student at NM-AIST who is carrying on a Ph. D research study to investigate the privacy and security of the biometric technology based on data from international passports in Uganda. Wish to request for a little of your time, for basic questions around the knowledge of the passport acquisition in Uganda. The answers you offer will be kept secret. The information you provide will improve the government understanding of how the seclusion and protection of the biometric passport can be raised.

May, 2018

Section A: Demographic and Passport Acquisition

Instruction: *Please tick (√) the option best describing your status from the values on the right-hand side (for A1).*

Question One

Parameters	**Values**
A1: Gender	☐ Male ☐ Female

Section B: Passport Issuance Process

Instruction: Please circle/state response that best identifies your case from the question below (from B1- B8*).*

Question Two

B1: Is access to security of Machine Readable Travel Documents (MRTD) production and issuance facilities controlled?

- ☐ Yes
- ☐ No
- ☐ Other specify

B2: Which security features of passport are important as stated by the International Civil Aviation Organization (ICAO)? (You can circle more than one response to this inquiry)

- ☐ Structure feature
- ☐ Substance feature
- ☐ Data feature
- ☐ Other specify

B3: What threats/attacks do you experience to the security of issuing passports (travel documents)? (You can tick (√) more than one response to this inquiry)

- ☐ Counterfeiting a travel document
- ☐ Photo substitution
- ☐ Substitution of entire page(s) or visas
- ☐ Impostors alter identity
- ☐ Other specify

B4: What efforts are required to mitigate the impacts of identity theft? (You can circle more than one response to this inquiry)

- ☐ Improve the integrity
- ☐ Improve the chances of identifying extremist
- ☐ Aid n recovery of national
- ☐ Other specify

B5: Is it appropriate for Government to use biometrics to verify identity for passports?

- ☐ Very suitable
- ☐ Neutral
- ☐ Not suitable
- ☐ Other specify

B6: Should biometric IDs be combined with other personal identifiers?

- ☐ Yes
- ☐ No
- ☐ Other specify

B7: Is it suitable for government to create a biometric database for serious offenders?

- ☐ Very suitable
- ☐ Suitable
- ☐ Neutral
- ☐ Not suitable

B8: Is biometric a better way of authenticating humans?

- ☐ Yes
- ☐ No
- ☐ Don't know
- ☐ Other specify

Section C: Security Issuance Process

Question three

C1: Is access to facilities/databases controlled?

- ☐ Yes
- ☐ No
- ☐ Other specify

C2: Which data elements do you consider when uploading information to the database. (Circle more than one answer)

- ☐ Travel document identification number
- ☐ Type of document (passport or other)
- ☐ Issuing State's ICAO Code
- ☐ Status of the document (i.e. Stolen blank)
- ☐ Country of theft (only mandatory for stolen blank travel documents).
- ☐ Other specify

C3: Does the country's TDIA staffs have access to databases to read, write the individual's biometric data?

- ☐ Yes
- ☐ No
- ☐ Other specify

C4: Who is responsible for the individual's biometric data in the database? (Circle more than one answer)

- ☐ Immigration officers
- ☐ Issuing officers
- ☐ Database administrator
- ☐ All staff members at the issuing offices
- ☐ Other specify

C5: How many stages are involved in the issuance process from submission of application to issue of passport?

- ☐ One
- ☐ Two
- ☐ Three
- ☐ Four
- ☐ Five
- ☐ Other specify

C6: What type of biometrics data do you use in the issuance process? (Circle more than one answer)

- ☐ Face Recognition
- ☐ Fingerprint Scan
- ☐ Irises Scan
- ☐ Voice Scan
- ☐ Signature Scan
- ☐ Hand Scan
- ☐ Other specify

C7: Why do you use the specific biometric data chosen in D11 above? (Circle more than one answer)

- ☐ Easy to use
- ☐ High-security components
- ☐ Complex to forge individual data
- ☐ Other specify

C8: Do you think the biometric template data are secrets and secure?

- ☐ Yes
- ☐ No
- ☐ Other specify

C9: Is the enrolled biometrics template data accessed by every member of the staff?

- ☐ Yes
- ☐ No

C10: Do you think anyone can create an image of the sample from the biometrics template data?

- ☐ It's possible
- ☐ Not possible
- ☐ Some features can be reverse engineered
- ☐ Other Specify

C11: How do you detect compromised template data? (Circle more than one answer)

- ☐ Sending signal to the authorized officer
- ☐ Alarming the authority for intrusion
- ☐ Blocking the IP for the access
- ☐ Other specify

C12: How do you handle tampered data? (Circle more than one answer)

- ☐ Investigate the entree route
- ☐ Replace the tempered data
- ☐ Extract the reserved copy
- ☐ Call the individual for another extracts
- ☐ Other specify

C13: Is there segregation of tasks throughout the issuance process, requiring at least two people to issue a passport?

- ☐ Yes
- ☐ No
- ☐ Other specify

C14: What are the commonly expressed fears regarding biometric data and privacy? (Circle more than one answer)

- ☐ Unauthorized Entree
- ☐ Information Disclosure
- ☐ Information Abuse
- ☐ Improper data transmission
- ☐ Other Specify

C15: How are people's/ Citizen's information being handled during passport acquisition?

(a) Is the individual biometric data given to government institutions for other purposes?

- ☐ Yes
- ☐ No
- ☐ Other specify

(b) Is the individual biometric data given to private institution without their consent?

- ☐ Yes
- ☐ No
- ☐ Other specify

C16: Do you think current biometrics data solutions can fulfil the requirements of border control regarding privacy and security of person's data?

- ☐ Yes
- ☐ No
- ☐ Need for e-passport control
- ☐ Other specify

Section D: Biometric System Database
Question Five

D1: Do you have cases of frequent lost or stolen passports?

- ☐ Yes
- ☐ No
- ☐ Other specify

D2: Do you investigate cases of frequent lost or stolen passports?

- ☐ Yes
- ☐ No
- ☐ Other specify

D3: Are data on lost and stolen travel documents sent to the national border authority?

- ☐ Yes
- ☐ No
- ☐ Other specify

D4: Are data on lost and stolen travel documents sent to regional watch list databases?

- ☐ Yes
- ☐ No
- ☐ Other specify

D5: Is biometric security levels be adjusted for specific transaction or process?

- ☐ Yes
- ☐ No
- ☐ Other specify

D6: What are the normally expressed attacks regarding the biometric passport issuance? (Circle more than one answer)

- ☐ Brute-force
- ☐ Password
- ☐ Denial of service
- ☐ Eavesdropping
- ☐ Others specify

D7: Are staffs trained in the detection of fraudulent documents?

- ☐ Yes
- ☐ No
- ☐ Other specify

D8: How are staffs trained in the detection of fraudulent documents?

- ☐ Spying
- ☐ Using sensor detection
- ☐ Other specify

D9: Is access to the issuing software and database restricted?

- ☐ Yes
- ☐ No
- ☐ Other specify

D10: Is access to the issuing software tracked and logged?

- ☐ Yes
- ☐ No
- ☐ Other specify

D11: Is the software mechanism effective in the detection of the fraudulent?

- ☐ Strongly effective
- ☐ Very Effective
- ☐ Not effective
- ☐ Ineffective
- ☐ Very ineffective

D12: What do you think is the best solution to prevent the fraudulent or the attack?

……
……
……
……

D13: State types of secrecy enhancing technologies legally offered for the citizen acquiring the Passport? (Circle more than one answer)

- ☐ Anonymous calling cards
- ☐ Encryption programmes
- ☐ Identity management
- ☐ Other specify

Section E: Challenges and Policy
Question Six

E1: Whom do you think must implement new safety technologies on passport?

……
……
……

E2: What security features would you suggest for the development and implementation of new biometric passport?

……
…….....

Thank You

Appendix 2: Quantitative questionnaires for document owners

Implemented by

Nelson Mandela African Institution of Science and Technology (NM-AIST)
School of Computational and Communication Science and Engineering

Consent Statement

I am a staff of Muni University currently student at NM-AIST who is carrying on a Ph. D research study to investigate the privacy and security of the biometric technology based on data from international passports in Uganda. Wish to request for a little of your time, for basic questions around the knowledge of the passport acquisition in Uganda. The answers you offer will be kept secret. The information you provide will improve the government understanding of how the seclusion and protection of the biometric passport can be raised.

May, 2018

Section A: Demographics

Instruction: Circle the number best describe your status from the values on the right-hand side (A1-A3).

Question One

Parameters	Values
A1: Gender	1=Male, 2=Female
A2: Age	1= 21–30, 2=30-60
A3: Professional	1= Student, 2= Teaching staff 3=Employee, 4= Other Specify

Section B: Passport Acquisition

Instruction: Circle the number best describe your case from the values on the right-hand side (B1-B5).

Question Two

B1: Do you own a Passport?	1= Yes, 2= No, 3= Other specify
B2: Type of passport issued?	1=Ordinary, 2=Diplomatic 3= Official, 4= East African, 5= Travel Documents, 6= Others
B3: Form in which passport is acquired	1= Normal, 2=Express, 3= Other specify
B4: Have you ever travelled overseas?	1=Yes, 2=No
B5: Purpose for your travel Overseas?	1=Tourist, 2=Business, 3= Health, 4= Education, 5= Sports, 6=Employment,7= Conference, 8=Citizenship, 9= Other

Section C: Technology used in Passport Acquisition

Instruction: Circle the number best describe your case from the values on the right-hand side (C1-C3).

Question Three

C1: Have you ever heard about Biometrics Technology?	1= Yes, 2= No 3= Don't Know
C2: What type of biometric technology do you know?	1=Fingerprints, 2=Facial, 3=Iris, 4=Palms Image, 5=Voice, 6=Giant, 7=Other specify
C3: Do you feel secure in giving your biodata to the Internal Affairs?	1= Yes, 2= No, 3= Not Sure

Section D: Passport Adoption and Usage

Question Four

D1-D14: Express your satisfaction in the passport security compliance by showing whether you Strongly Agree (SA), Agree (A), Neither Agree nor Disagree (U), Disagree (D) and Strongly Disagree (SD) by placing a tick (X) in appropriate box where SA=5, A=4, U=3, D=2 and SD=1.

Questions	**Strongly Disagree (1)**	**Disagree (2)**	**Uncertain (3)**	**Agree (4)**	**Strongly Agree (5)**
I feel biometric technologies are more secure than traditional IT security methods.					
Security of humanity is absolutely dependent on the growth and utilization of new safety technologies.					
Privacy should not be violated without reasonable suspicion of criminal intent.					
Uncomfortable to be under surveillance, even though you have no criminal intent.					
Novel safety technologies are likely to be abused by criminals					
Storage of data (e.g. Fingerprints or DNA samples) of all citizens in a central database are acceptable step to fight crime.					
The use of the biometric passport (e.g., fingerprint verification, facial recognition, iris recognition, and voice verification) makes me feel self-doubting because of the risk of my biometric data being stolen.					
It's a good chance to replace ordinary biometric passports with e-passport for security purpose.					
The biometric-based solutions are appropriate solution to fraud?					
Directors at the institutions should store all data they find necessary for security reasons					

as long as they consider it necessary.					
Secrecy enhancing technologies are a necessity in today's society to preserve privacy.					
Gathering of personal data from unsuspicious individuals must be anonymous until identification is authorized by court order.					
Authorized personnel can have access to collected personal data.					
Implementing new security technologies must be checked for privacy impact.					
Usage of biometric passport technology.					

D15:

Factors Influencing the Adoption and usage of Biometric Technology	**Strongly Disagreed (1)**	**Disagreed (2)**	**Uncertain (3)**	**Agreed (4)**	**Strongly Agreed (5)**
Protect Frauds					
Provide Security					
Identify individual					
Monitor crimes					
Privacy invasion					

Section E: Users fear, concerns and challenges

Instruction: Please circle the number best describing your case from the values (for E1-E).

Question Five

E1: What are the commonly expressed fears regarding biometric data and privacy? (Circle more than one answer)

- ☐ Unauthorized Access
- ☐ Information Disclosure
- ☐ Information Abuse
- ☐ Improper data Transmission
- ☐ Other Specify

E2: Which biometrics technology would you be comfortable to use in border point? (Circle more than one answer)

- Face trait
- Irises Scan
- Finger Scan
- Voice Scan
- Signature Scan
- Hand Scan
- Keystroke Scan
- Other Specify

E3: In your opinion, what are the main influencing factors for biometric deployment in border controls? (Circle more than one answer)

- Protects from crime and frauds
- Provides security
- Identifying and authenticating individuals
- Control access to workplaces
- Ensuring uniqueness of individuals.
- Speed up and verify the identity
- An invasion of privacy?
- Constant monitor and surveillance
- Other Specify

E4: State privacy enhancing technologies should be legally available for all citizens acquiring the Passport? (You can circle more than one answer to this question)

- Anonymous calling cards
- Encryption programmes
- Identity management
- Other Specify

E5: Which factor do you think can de-motivated one not to acquire passport?

- Security
- Privacy
- Unauthorized access or disclosure
- High cost
- Bureaucratic procedures
- Signature collection
- inconvenience
- Other Specify

E6: What are the challenges you think exist in acquiring passport?

- High Cost
- Delays in processing
- Bureaucratic, bribe and corruption
- Centralization of processing office
- Insecurity and Duplication of data
- Others Specify

E7: What protection mechanisms would you suggest protecting people's data acquiring passport?

- ☐ Encryption techniques
- ☐ Reduce levels of access to database
- ☐ Building data centres
- ☐ Others specify

Section F: Policy

Question Six

F1: What policy reforms do you think are needed to improve the passport acquisition situation?

- ☐ Centralization
- ☐ Decentralization
- ☐ Eliminating tribalism, corruption
- ☐ Use district headquarters to issue ePassport
- ☐ Other specify

F2: Who should implement new safety technologies?

- ☐ The citizens Country
- ☐ Local leader
- ☐ Government and law marker
- ☐ Security experts and intelligence
- ☐ Others specify

F3: What your comments regarding regulation of expansion and implementation of new safety technologies?

- ☐ Laws to protect information about the users
- ☐ Sensitization of citizens about new security and safety of information
- ☐ Legal procedure for wrong or misuse of information
- ☐ keep the personal data as secure as possible
- ☐ Others specify

F4: Any other remarks?

……
……
……
……

Thank You

Appendix 3: Introduction letter from the school of CoCSE

THE NELSON MANDELA
AFRICAN INSTITUTION OF SCIENCE AND TECHNOLOGY
(NM-AIST)
School of Computational and Communication Science and Engineering

Direct Line: +255 272970001
Fax: +255 272970016
E-mail: dean-cocse@nm-aist.ac.tz

Tengeru
P.O. Box 447
Arusha, TANZANIA
Website: www.nm- aist.ac.tz

OUR Ref.No. NM-AIST/P. 216/UG.16/07 **Date:** 19th October, 2017

To Whom It May Concern,

RE: INTRODUCTION FOR MR. TABAN HABIBU

I wish to introduce Mr. Taban Habibu (Reg. No. P.216/UG.16) who is pursuing PhD degree in Mathematical and Computer Science and Engineering, specializing in Computer Science and Engineering by research and thesis mode at NM-AIST.

As part of the requirement for PhD degree, Mr. Taban has already defended his research proposal successfully and now he is undertaking a research with title ***"Development of Enhanced Privacy and Security Template of Bio-metric Technology".***

In order to accomplish the research objectives, Mr. Taban would like to collect some data/information from your Institution/Organization. The data/information collected will be used for Research purposes only.

It is my sincere hope that you will assist Mr. Taban in accomplishing his research.

Looking forward to your positive cooperation.

Sincerely,

Shubi Kaijage,*PhD*
Ag. Dean,School of CoCSE

Nelson Mandela African Institute of Science and Technology (NM-AIST - ARUSHA) P. O. Box 447 Tel: +255 27 255507

Appendix 4: Introduction letter from the office of Deputy Vice Chancellor

MUNI UNIVERSITY

OFFICE OF THE DEPUTY VICE CHANCELLOR
(ACADEMIC AFFAIRS)

P.O. Box 725Arua, Uganda
Tel: +256 476 420312/3/4; Fax: +256 476 420316
Email: dvc@muni.ac.ug
www.muni.ac.ug

Our Ref: **MU/CR/200/220/1**
Your Ref: .....

19th February, 2018

Permanent Secretary
Ministry of Internal Affairs
P.O Box 7165 / 7191, Kampala

Dear Sir / Madam,

RE: INTRODUCTION LETTER FOR MR. TABAN HABIBU

I wish to introduce Mr. Taban Habibu who is an employee of Muni University at the Department of Computer and Information Science, Faculty of Technoscience. He is currently pursuing a PhD study at the Nelson Mandela African Institution of Science and Technology (NM-AIST) Arusha Tanzania.

As part of his requirement for PhD degree, he is undertaking a research entitled "***Development of enhanced privacy and security template of Bio-Metric technology***" based on international passports.

In order to accomplish the research objectives, Mr. Taban Habibu would like to collect some information from your institution/organization. The information collected will be used for research purposes only.

It is our sincere hope that you will accord Mr. Taban Habibu the necessary information in accomplishing his research.

Looking forward to your positive consideration.

Thank you.

MUNI UNIVERSITY
P.O.BOX 725 ARUA
19 FEB 2018
OFFICE OF THE DEPUTY VICE CHANCELLOR

Yours sincerely,

Dr. Simon K. Anguma
Assoc Prof of Physics
Deputy Vice Chancellor (Academic Affairs)

Appendix 5: Python code for account creation, Login and template rendering

```
  from flask import (
     Blueprint,
     request,
     session,
     redirect,
     url_for,
     render_template,
     send_file,
     send_from_directory
     )
  from jinja2 import (
     Environment,
     FileSystemLoader
     )
  import os
  env = Environment(
        loader=FileSystemLoader(
           'app/blue_prints/home/templates'
           )
        )
  bp_create_user = Blueprint(
     'create_user',
     __name__
     )

      #----------------------helper imports---------------------------------
from .helpers import (
   create_user as bp_helper
   )
#----------------------form imports---------------------------------
from .forms import(
   create_user as forms
   )
#------------------General utility-------------------------------------
from blue_prints.utils import (
   current_user as current_user_utils,
   request_formatter as request_utils
   )

@bp_create_user.route("/create_user")
def create_user():
   if "e-passport-user-name" in session:
      if session['e-passport-user-role']=="head-quater":
         return redirect(
            url_for(
               "head_quater.head_quater_home"
               )
```

```
            )
    elif session['e-passport-user-role']=="applicant":
        return redirect(
            url_for(
                "applicant.applicant_home"
                )
            )
    elif session['e-passport-user-role']=="regional-office":
        return redirect(
            url_for(
                "regional_officer_home.regional_officer_home"
                )
            )
regional_offices=bp_helper.AvailableRegionalOffices()
regional_offices=regional_offices()
createUserForm=forms.CreateUser()
createUserForm.populateOfficeIdChoices(
    regional_offices=regional_offices
    )
tmpl = env.get_template(
            'create_user/__init__.html'
            )
return tmpl.render(
            title="Create user",
            createUserForm=createUserForm
            )
```

Appendix 6: Python code for biometric feature Scanning

```
from flask import (
    Blueprint,
    request,
    session,
    redirect,
    url_for,
    render_template,
    send_file,
    send_from_directory
    )
from jinja2 import (
    Environment,
    FileSystemLoader
    )
import os
env = Environment(
        loader=FileSystemLoader(
            'app/blue_prints/head_quater/templates'
            )
        )
bp_biometric_scan = Blueprint(
    'biometric_scan',
    __name__
    )

#----------------------helper imports---------------------------------
from .helpers import (
    biometric_scan as bp_helper
    )
#----------------------form imports-----------------------------------
from .forms import(
    biometric_scan as forms
    )
#------------------General utility-------------------------------------
from blue_prints.utils import (
    current_user as current_user_utils,
    request_formatter as request_utils,
    passport as passport_utils
    )

class POSTKwargs(object):
    """docstring for POSTKwargs"""

    def __init__(self, request):
        super(POSTKwargs, self).__init__()

        self.request = request
```

```
    def __call__(self):

        kwargs=dict()
        for a in list(self.request.form):
            kwargs[a]=self.request.form[a]
        return kwargs

@bp_biometric_scan.route(
    "/face_scan_get/<applicant_id>",
    methods=["POST"]
    )
def face_scan_get(applicant_id):
    if "e-passport-user-name" in session:
        if session['e-passport-user-role']=="head-quater":
            try:

save_changes=current_user_utils.RemoveDecryptedPassportPhotoOfficer(
                            username=session["e-passport-user-name"]
                            )
                save_changes()
            except:
                pass
            kwargs={
                    "document":request.files["webcam"],
                    "description":"Passport Photo",
                    "applicant_id":applicant_id
                    }
            save_changes=bp_helper.SaveFingerPrint(
                        **kwargs
                        )
            save_changes()
            return "Saved"
            # tmpl = env.get_template(
            #             'biometric_scan/__init__.html'
            #             )
            # return tmpl.render(
            #             title="Biometric scan",
            #             passport_code=passport_code,
            #             document_state=document_state,
            #             # applicantDocumentForm=applicantDocumentForm,
            #             # decryptForm=decryptForm,
            #             #
addApplicantDocumentDetail=addApplicantDocumentDetail,
            #             finger_print_state=finger_print_state
            #             )
        elif session['e-passport-user-role']=="applicant":
            return redirect(
                url_for(
                    "applicant_home.applicant_home"
```

```
                )
            )
    elif session['e-passport-user-role']=="regional-office":
        return redirect(
            url_for(
                "regional_office_home.regional_office_home"
                )
            )
return redirect(
    url_for(
        "home.login"
```

Appendix 7: Python code for facial extraction and encryption-decryption process

```
<div class="main-content">
<section class="mod-text mod-intro content-section">
   <div class="wrapper">
      <div class="row">
         <h3 style="text-align: center; color: maroon"><b>PASSPORT
APPLICATIONS </b></h3>
         <hr><br>
         <div class="col-md-12 col-xs-12">
         <a
href="view_details_head_quater?applicant_id={{applicantDocumentForm.appl
icant_id.data}}" >Go back to view details </a>
            <!-- CSS -->
<script src="static/js/webcam.js" type="text/javascript" charset="utf-8" async
defer></script>
<style>
#my_camera{
 width: 250px;
 height: 250px;
 border: 1px solid #cccfee;
}
</style>


 <!-- Script -->

 <!-- Code to handle taking the snapshot and displaying it locally -->
 <script language="JavaScript">

 // Configure a few settings and attach camera
 function configure(width,height){
  Webcam.set({
   width: width,
   height: height,
   image_format: 'jpeg',
   jpeg_quality: 90
  });
  Webcam.attach( '#my_camera' );
 }
 // A button for taking snaps

 // preload shutter audio clip
 var shutter = new Audio();
 shutter.autoplay = false;
 shutter.src = navigator.userAgent.match(/Firefox/) ? 'shutter.ogg' :
'shutter.mp3';

 function take_snapshot() {
  // play sound effect
```

```
 shutter.play();
 // take snapshot and get image data
 Webcam.snap( function(data_uri) {
 // display results in page
 document.getElementById('results').innerHTML =
  '<img id="imageprev" src="'+data_uri+'"/>';
 } );

 Webcam.reset();
}

function saveSnap(){
 // Get base64 value from <img id='imageprev'> source
 var base64image = document.getElementById("imageprev").src;
 var url='face_scan_get/{{applicantDocumentForm.applicant_id.data}}';
 console.log(url);
// var ajax = new XMLHttpRequest();
//  ajax.open("POST",url,false);
//  ajax.setRequestHeader('Content-Type', 'application/upload');
//  ajax.send(base64image );
//  alert('done');

 Webcam.upload( base64image, url, function(code, text) {
    console.log(base64image);
    console.log(code);
    console.log(text);
  console.log('Save successfully');
  location.reload();
  //console.log(text);
 });

}

</script>
              {% include "biometric_scan/form.html" %}
           </div>
        </div>
    </div>
</section>
</div>

form interface

<div class="row">
<div class="col-lg-12 col-md-12 col-sm-6 col-xs-6">
{% if decryptForm.password.errors %}
    {% for error in decryptForm.password.errors %}
        <span style="color: red; text-align: center;">
            {{error}}
        </span><br>
```

```
    {% endfor %}
{% endif %}

<form action="biometric_scan_decrypt_upload" method="POST" accept-
charset="utf-8">
                {{
                   decryptForm.password(
                      placeholder="Password",
                      class="form-control",
                      style="margin-bottom: 2px;"
                      )
                }}
                {{
                   decryptForm.applicant_id
                }}
                <button type="submit" class="btn">Decrypt</button>
             </form>
             <hr>
{% if applicantDocumentForm.document.errors %}
   {% for error in applicantDocumentForm.document.errors %}
      <span style="color: red; text-align: center;">
         {{error}}
      </span><br>
   {% endfor %}
{% endif %}
{% if addApplicantDocumentDetail %}
   {% if addApplicantDocumentDetail==1 %}
      <span class="alert alert-success">
         Document successfully added!
      </span><br>
   {% endif %}
{% endif %}
</div>
<div class="col-lg-6 col-md-6 col-sm-6 col-xs-6">
<h3>Upload new passport photo</h3>
<img src="static/images/encrypted/{{document_state[1]['Passport
Photo']}}.png" width="100" height="100" style="min-height: 100px;"
class="img-thumbnail img-responsive">
<hr>
<form action="face_scan" method="POST" accept-charset="utf-8"
enctype="multipart/form-data">
   {{
             applicantDocumentForm.document(
                accept="image/*"
                )
          }}
          {{
             applicantDocumentForm.applicant_id
          }}
```

```
        <button type="submit" class="btn btn-primary" style="margin-top:
2px;">
        Upload new passport photo
        </button>
</form>
<button type="button" class="btn btn-dark" style="margin-top: 2px;" data-
toggle="collapse" data-target="#webcam-capture">
   Webcam
   </button>
</div>
<div class="col-lg-6 col-md-6 col-sm-6 col-xs-6">
<h3>Upload finger print scan</h3>
{% if finger_print_state==True %}
      <img src="static/images/encrypted/{{document_state[1]['Finger
Print']}}.png" width="100" height="100" class="img-thumbnail img-
responsive" style="min-height: 100px;">
      {% else%}
      No finger print uploaded
      {% endif %}
<hr>
<form action="finger_print_scan" method="POST" accept-charset="utf-8"
enctype="multipart/form-data">
   {{
            applicantDocumentForm.document(
               accept="image/*"
               )
         }}
         {{
            applicantDocumentForm.applicant_id
         }}
         <button type="submit" class="btn btn-primary" style="margin-top:
2px;">
         {% if finger_print_state==True %}
         Upload new finger print scan
      {% else %}
         Upload finger print scan
      {% endif %}
         </button>
</form>
</div>
</div>
<hr>
{% include "biometric_scan/webcam.html" %}
```

Appendix 8: Python code for Cryptography key generation

```
from cryptography.fernet import Fernet, MultiFernet
key1 = Fernet(Fernet.generate_key())
key2 = Fernet(Fernet.generate_key())
f = MultiFernet([key1, key2])
token = f.encrypt(b"Secret message!")
token

b'...'
f.decrypt(token)
b'Secret message!'
key3 = Fernet(Fernet.generate_key())
f2 = MultiFernet([key3, key1, key2])
rotated = f2.rotate(token)
>>> f2.decrypt(rotated)
b'Secret message!'
```

Appendix 9: Python code for encryption algorithm process

```
            if not data:
                break
            pdf=open(file_path_decrypted, 'wb')
            pdf.write(data)
            pdf.close()
Key1_bytes=fernet.generate_ key()
Key1= Fernet(Key1_bytes)
Key2_bytes=KEY_2_BYTES
Key2= Fernet(Key2_bytes)
f=Multifernet ([Key1, Key2])
file=open(file_path-decrypted, 'rb')
while True:
            data=file.read()
            if not data:
                break
            out_file=open(file_path_encrypted, 'wb')
            token =f.encrypt(data)
            out_file.write(token)
            out_file.close()
encrypted_key_one=Key2.encrypt(Key1_bytes)
encrypted_Key1=open(file_path_keys, ''w")
encrypted_Key1.write(encrypted_key_one.decode())
encrypted_Key1.close()
file.close()
os.remove()
            file_path_decrypted
            )
            session.close()
            return True

class Documentstate(object)
```

Appendix 10: Python code for decryption algorithm process

```
print(applicant_document.document_id)

file_path_decrypted=f"{os.getcwd()}/app/blue_prints/static/images/decrypted_t
emp/{applicant_document.document_id}.png"

file_path_encrypted=f"{os.getcwd()}/app/blue_prints/static/images/encrypted/{
applicant_document.document_id}.png"

file_path_keys=f"{os.getcwd()}/app/blue_prints/static/images/keys/{applicant_
document.document_id}.txt"
    key1_decoded=open(file_path_keys,"r")
    key1_encoded=key1_decoded.readline().encode()
    key2_bytes=KEY_2_BYTES
    key2 = Fernet(key2_bytes)
    decrypted_key1=key2.decrypt(key1_encoded)
    key1_bytes=decrypted_key1
    key1 = Fernet(key1_bytes)

    f = MultiFernet([key1, key2])
    file_2=open(file_path_encrypted,"rb")
    while True:
       data1=file_2.read()
       if not data1:
          break
       decrypted_file=open(file_path_decrypted,"wb")
       token = f.decrypt(data1)
       decrypted_file.write(token)
       decrypted_file.close()
    file_2.close()
    key1_decoded.close()
    session.close()
    return True
```

Appendix 11: Python code for Database model settings

```
from sqlalchemy import Column, Integer, String, ForeignKey, Table
from sqlalchemy.orm import relationship
from sqlalchemy.ext.declarative import declarative_base
Base = declarative_base()
class User(Base):
__tablename__ = 'user'
import os,os.path
from passlib.hash import sha256_crypt
import time
import models
from models.utils.db_config import (
   CONFIG,
   DB_PATH
   )
from models.utils import dbConfig

class DBCheck(object):
   """docstring for DBCheck"""
   def __init__(self):
      super(DBCheck, self).__init__()

      if not os.path.exists(f"{DB_PATH}"):
         print(u"database does not exist.\n Generating a new database
schema...")
         dbConfig.Base.metadata.create_all(dbConfig.engine)
         password=u"habib@2019"
         hashed = sha256_crypt.encrypt(password)
         session=dbConfig.Session()
         default_user=models.User(
                  username=u"admin@e-passport.com",
                  role=u"head-quater",
                  password=hashed
                  )
         session.add(default_user)
         session.commit()
         session.close()

         print(u"Database Successfully set...")
         time.sleep(2)
```

Appendix 12: Python code for biometric template and biodata encryption

```
from .encrypt_decrypt import(
    DecryptImage,
    EncryptImage
    )

__all__=(
    DecryptImage,
    EncryptImage
    )

     spif_decrypt
        )
    spif_decrypt(
        "DETF.py",
        "1.txt",
        "2.png",
        0,
        "-m"
        )

   spif_decrypt,
    spif_encrypt
    )

class DecryptImage(object):
    """docstring for DecryptImage"""

    def __init__(self, **kwargs):
        super(DecryptImage, self).__init__()

        self.decryption_and_encryption_table =
kwargs['decryption_and_encryption_table']
        self.input_file_path=kwargs['input_file_path']
        self.output_file_path=kwargs['output_file_path']
        self.mute="-m"
        self.encryption_level=0

    def __call__(self):

        spif_decrypt(
            self.decryption_and_encryption_table,
            self.input_file_path,
            self.output_file_path,
            self.encryption_level,
            self.mute
            )
```

```
class EncryptImage(object):
    """docstring for EncryptImage"""

    def __init__(self, **kwargs):
        super(EncryptImage, self).__init__()

        self.decryption_and_encryption_table =
kwargs['decryption_and_encryption_table']
        self.input_file_path=kwargs['input_file_path']
        self.output_file_path=kwargs['output_file_path']
        self.mute="-m"
        self.encryption_level=0

    def __call__(self):

        spif_encrypt(
            self.decryption_and_encryption_table,
            self.input_file_path,
            self.output_file_path,
            self.encryption_level,
            self.mute
            )
```

Appendix 13: Python code for Twilio SMS

```
from twilio.rest import Client
account_sid = 'ACXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX'
auth_token = 'your_auth_token'
client = Client(account_sid, auth_token)

message = client.messages \
    .create(
            body='Hi there!',
            from_='+256xxxxxxx',
            to='+256xxxxxxxx'
            )

print(message.sid)
```