A Conceptual Technique for Deriving Encryption Keys from Fingerprints to Secure Fingerprint Templates in Unimodal Biometric Systems

Joseph Mwema
School of Computing and Information Technology (SCIT)
Jomo Kenyatta University of Agriculture and Technology
JKUAT
P. O. Box 62000 - 00200
Nairobi, Kenya

Stephen Kimani, Ph.D
School of Computing and Information Technology (SCIT)
Jomo Kenyatta University of Agriculture and Technology
JKUAT
P. O. Box 62000 - 00200
Nairobi, Kenya

Michael Kimwele, Ph.D
School of Computing and Information Technology (SCIT)
Jomo Kenyatta University of Agriculture and Technology
JKUAT
P. O. Box 62000 - 00200
Nairobi, Kenya

ABSTRACT
In this study, we reviewed biometric template protection schemes in subsisting literature and established that there is no reliable, efficacious and foolproof technique that assures diversity, revocability, security and optimal performance as is required of an ideal biometric template security scheme. This status of affairs motivated us to contrivance an approach that derives biometric encryption keys from biometric fingerprint templates. The technique we proposed involves a two-step enrollment and authentication of fingerprints while encrypting fingerprint templates with encryption keys derived from other biometric fingerprint templates before archiving them to a database. The system was implemented using Java, developed on Netbeans 8.0 IDE, MySQL RDBMS was used for back-end database and utilized Source AFIS java library framework for fingerprint verification and identification. Test results were carried out to determine the system's efficacy.

General Terms
Pattern Recognition, Security, Algorithms, Technique.

Keywords
Biometric, Fingerprint, Template, Security, Encryption, Decryption, Key, Source AFIS, AES, Java, Technique.

1. INTRODUCTION
Various approaches and techniques of securing biometric templates have been proposed and researched on. In this study we majorly explored biometric template encryption and feature transformation techniques. We discovered that most of the current biometric template protection techniques seek to address security of biometric templates in multimodal biometric systems which are expensive and a preserve of affluent regimes and security agencies. Unimodal biometric systems on the other hand like 'biometric fingerprints only systems' are frugal and easy to implement but without a distinctively secure way of guaranteeing the safety of their biometric fingerprint templates in biometric system's databases. This research sought to establish an approach for securing biometric templates in unimodal biometric fingerprint systems' databases by proposing to encrypt biometric fingerprint templates with encryption keys generated from other biometric fingerprints using a two-step fingerprint enrolment and authentication process [3].

2. REVIEW OF EXISTING BIOMETRIC TEMPLATE PROTECTION TECHNIQUES
According to an antecedent research review by Mwema et al in [2] we observed that the existing theoretical literature categorizes biometric template protection schemes largely into ***feature transformation*** and ***biometric encryption***. Schemes and approaches documented under these two categories and identified by existing literature in feature transformation are the ***invertible*** *bio-hashing* and the ***non-invertible*** *cancellable biometrics* while under biometric encryption's ***key binding*** there is *fuzzy vault* and *fuzzy commitment*. *Secure sketches* and *fuzzy extractors* were identified as ***key generation*** methods under biometric encryption techniques. The other biometric template protection schemes that do not virtually fall under these two categories which are used in securing fingerprint templates are *watermarking, AES, RSA* and *ECC algorithms*.

In this study we explored these biometric template protection schemes and identified the following inadequacies and shortcomings. We established from studying *cancellable biometrics* scheme that, if transformational parameters are leaked or known to hackers, the adversaries will be able to do cross matching of fingerprint templates across databases [4]. High variances resulting from transformation of biometric data in cancellable biometrics schemes results in reduced verification and identification speeds [5]. *Bio-hashing* scheme on the other hand suffers from possibilities of information leakage in instances of calculating bio-hash [6] and reduced performance in cases like when much time is spent in probing for legitimate tokens presented by adversaries purporting to be authentic fingerprint bearers [7]. Analysis on reusability of *secure sketches and fuzzy extractors*' scheme implored that they could not be safely applied severally on the same biometric template thus considerably restraining and decreasing their functional practicality in biometric systems [8].

In other schemes, a *Fuzzy vault* scheme to start with has a difficulty in revoking a compromised vault which is prone to crossmatching and secondly, it is possible to stage attacks if fuzzy vault points are statistically analyzed. The other downside of a fuzzy vault is that it is possible to glean over users' fingerprint templates if they are ephemerally exposed in a fuzzy vault scheme [9]. While exploring *Fuzzy Commitment* scheme, it was observed that an ordinary Fuzzy commitment scheme does not guarantee satisfactory hiding and binding of biometric fingerprint traits and is also considered insecure as

pointed out by Al-Saggaf & Acharya [10]. Studying use of *RSA and ECC algorithms* in securing biometric templates from adversary attacks exposed the considerable amount of time taken by these algorithms in decryption of images during authentication processes of enrolled persons [11]. In the end while concluding the review of subsistent biometric template protection techniques we observed that in *Watermarking Scheme*, a significant amount of time is required to insert a watermark into a biometric fingerprint image and that most watermarking algorithms needed the availability of the original image to extract the watermark. This additional requirement for storage of the pristine image in watermarking scheme would prompt for need to allocate more database space when using watermarking scheme which is not the case with other biometric template protection schemes [12].

3. BIOMETRIC FINGERPRINT TEMPLATE ENCRYPTION CONCEPT

3.1 Biometric Encryption Introduction

In a recent study of measures and approaches used to secure biometric fingerprint templates by Mwema et al in [13] it was established that encryption of biometric fingerprint templates was the most sought after technique among biometric systems developers in ascertaining security of biometric templates before archiving them. Das in [1] emphasized that the advantage of using biometric keys as compared to other traditional forms of identification like password is;

i. Biometric Keys cannot be misplaced or forgotten.

ii. It is difficult to copy and distribute them.

iii. They are extremely hard to reverse engineer, forge or distribute

iv. They are not easy to guess at unlike passwords.

This section will demonstrate the adaptive and robust approach we used to derive biometric encryption keys from biometric fingerprint templates. First, when a fingerprint is captured using a fingerprint sensor, a fingerprint template $\mathbf{B_T}$ is extracted from it for purposes of enrollment, verification and identification.

3.2 Description of Biometric Fingerprint Encryption Key Components

$\mathbf{B_T}$ will denote a biometric fingerprint template.

A biometric fingerprint template $\mathbf{B_T}$ consists of minutiae **m** points as shown below;

$$\Sigma \mathbf{m_n} = \mathbf{m_{1+}}\ \mathbf{m_2} + \mathbf{m_3} +\ldots\ldots\ldots + \mathbf{m_n}$$

The encryption algorithm required the summation of ridges **r** in a biometric fingerprint template $\mathbf{B_T}$ which we calculated as follows;

$$\Sigma \mathbf{r_n} = \mathbf{r_{1+}}\ \mathbf{r_2} + \mathbf{r_3} +\ldots\ldots\ldots + \mathbf{r_n}$$

The encryption algorithm required the summation of minutiae **x** coordinate values in biometric fingerprint template $\mathbf{B_T}$ which we calculated as follows;

$$\Sigma \mathbf{x_n} = \mathbf{x_{1+}}\ \mathbf{x_2} + \mathbf{x_3} +\ldots\ldots\ldots + \mathbf{x_n}$$

The encryption algorithm required the summation of minutiae **y** coordinate values in Biometric Fingerprint Template $\mathbf{B_T}$ which we calculated as follows;

$$\Sigma \mathbf{y_n} = \mathbf{y_{1+}}\ \mathbf{y_2} + \mathbf{y_3} +\ldots\ldots\ldots + \mathbf{y_n}$$

The encryption algorithm required the summation of minutiae **θ** angle of orientation values in Biometric Fingerprint Template $\mathbf{B_T}$ which we calculated as follows;

$$\Sigma \boldsymbol{\theta_n} = \boldsymbol{\theta_{1+}}\ \boldsymbol{\theta_2} + \boldsymbol{\theta_3} +\ldots\ldots\ldots + \boldsymbol{\theta_n}$$

The encryption algorithm required the summation of all ridge bifurcations **b** in a given biometric fingerprint template $\mathbf{B_T}$ which we calculated as follows;

$$\Sigma \mathbf{b_b} = \mathbf{b_{1+}}\ \mathbf{b_2} + \mathbf{b_3} +\ldots\ldots\ldots + \mathbf{b_b}$$

The encryption algorithm required the summation of all ridge endings **e** in a given biometric fingerprint template $\mathbf{B_T}$ which we calculated as follows;

$$\Sigma \mathbf{e_e} = \mathbf{e_{1+}}\ \mathbf{e_2} + \mathbf{e_3} +\ldots\ldots\ldots + \mathbf{e_e}$$

A ridge type $\mathbf{r_i}$ is either a ridge ending $\mathbf{e_i}$ where **i = 1...e** or a bifurcation $\mathbf{b_k}$ where **k= 1...b**

All ridges $\mathbf{R_T}$ in a biometric template is a sum of all bifurcations $\Sigma \mathbf{b_b}$ and endings $\Sigma \mathbf{e_e}$ in a biometric template $\mathbf{B_T}$ as shown below;

$$\mathbf{R_T} = \Sigma \mathbf{b_b} + \Sigma \mathbf{e_e}$$

A biometric template $\mathbf{B_T}$ has minutiae points' $\mathbf{m_{1+}}\ \mathbf{m_2} + \mathbf{m_3} +\ldots\ldots\ldots + \mathbf{m_n}$ and ridges $\mathbf{R_T}$ such that

$$\mathbf{B_T} = \mathbf{m_{1+}}\ \mathbf{m_2} + \mathbf{m_3} +\ldots\ldots\ldots + \mathbf{m_n}$$

$$\mathbf{B_T} = \Sigma \mathbf{m_n}$$

A minutia point $\mathbf{m_i}$ is uniquely identified by

$\mathbf{m_i} = \{\mathbf{x_i}, \mathbf{y_i}, \boldsymbol{\theta_i}, \mathbf{r_i}\}$ where **i = 1..n**. as shown in [15].

3.3 Deriving Biometric Fingerprint Encryption Key

A biometric encryption key $\mathbf{Enc_k}$ is derived from a biometric fingerprint template's $\mathbf{B_T}$ total number of **x** values $\Sigma \mathbf{x_n}$, total number of **y** values $\Sigma \mathbf{y_n}$, summation of angles of orientation $\Sigma \boldsymbol{\theta_n}$, total number of ridge bifurcations $\Sigma \mathbf{b_b}$ and total number of ridge endings $\Sigma \mathbf{e_e}$ appended with alphanumeric literals in between them to increase the strength of the derived biometric encryption key as follows;

$\Sigma \mathbf{x_n}$ is appended with alphabet **'X'** and

$\Sigma \mathbf{y_n}$ is appended with alphabet **'Y'** and

$\Sigma \boldsymbol{\theta_n}$ is appended with alphabets **'AO'** and

$\Sigma \mathbf{b_b}$ is appended with alphanumeric **'BFN1'** and

$\Sigma \mathbf{e_e}$ is appended with alphanumeric **'END0'**

such that if $\Sigma \mathbf{x_n}$ is **1122**, $\Sigma \mathbf{y_n}$ is **3344**, $\Sigma \boldsymbol{\theta_n}$ is **5566**, $\Sigma \mathbf{b_b}$ is **77** and $\Sigma \mathbf{e_e}$ is **88** then the derived encryption key $\mathbf{Enc_k}$ will be as shown below

$$\mathbf{Enc_k = \{1122X3344Y5566AO77BFN188END0\}}$$

Encryption Key $\mathbf{Enc_k}$ derived from a Biometric Fingerprint Template $\mathbf{B_T}$ was thus arrived at using this novel approach shown below;

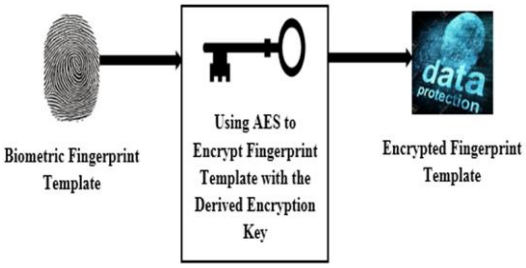
$\mathbf{Enc_k}$= $\Sigma \mathbf{x_n}$ & 'X' & $\Sigma \mathbf{y_n}$ & 'Y' & $\Sigma \boldsymbol{\theta_n}$ & 'AO' & $\Sigma \mathbf{b_b}$ & 'BFN1' & $\Sigma \mathbf{e_e}$ & 'END0'.

3.4 Advanced Encryption Standard (AES) Cypher Algorithm

The study adopted AES algorithm to encrypt and decrypt biometric fingerprint templates using the novel algorithm key we came up with. AES speeds are fast and the speeds also depends on the key size. AES is more secure when compared to other algorithms. AES can implement keys of sizes 128, 192 and 256 bits. This study used a 256 bit encryption. The fact that AES can allow for 256 bit keys is a significant strength that it has the potential of forefending against future attacks e.g. collision attacks and possible quantum computing algorithms [16].

In the end, the implemented biometric fingerprint encryption tool was as shown in *Figure 1* below.

Figure 1: Biometric Template Encryption



4. SYSTEM DESIGN AND DEVELOPMENT

This section will present the design and development process of the biometric fingerprint encryption and decryption tool.

4.1 Requirement Analysis

The Requirements of the biometric fingerprint encryption and decryption system tool were classified into *Functional Requirements* and *Non-Functional Requirements*.

4.1.1 Functional Requirements

Consequential requisites of the developed system comprised of the following;

i. System captures fingerprint images from biometric fingerprint images.

ii. System extracts fingerprint templates into ISO 19794-2 format and raw images.

iii. System has enrollment functionality of fingerprint templates into system database

iv. System has verification functionality of saved fingerprints from presented fingerprints.

v. System has identification functionality of saved fingerprints from presented fingerprints.

vi. System saves fingerprints in RDBMs

vii. System does encryption and decryption of users fingerprint templates.

viii. System derives encryption keys from enrolled fingerprints.

ix. System encrypts extracted fingerprint templates before saving to database with encryption keys derived from other fingerprints.

x. System performs decryption of archived encrypted fingerprint templates using decryption keys derived from enrolled user's fingerprint templates during verification and identification of enrolled system users.

xi. System uniquely identifies and verifies users after verification and identification of their presented fingerprints.

xii. System should not allow cross matching of fingerprints across various databases.

xiii. System should prevent reverse engineering of fingerprint template to obtain original fingerprint.

xiv. System matching speeds during verification and identification should not compromise system's False Acceptance Rate (FAR) and False Rejection Rate (FRR).

4.1.2 Non-Functional Requirements

The following are requisites that are not categorical to the main functionality of the main system but they enhanced usability, interactivity and presentation of fingerprint images and minutiae data. They are;

i. Intuitive and easy to use system user interface.

ii. Tabulated fingerprint minutiae data.

iii. Animated fingerprint image showing fingerprint patterns on presentation of fingerprint to sensor.

iv. System response turnaround time to users' interaction is within 1 minute.

v. System should be able to manually load fingerprint image files from computer data folders.

vi. System is not resource intensive as it is a light weight application.

vii. System uses various fingerprint readers.

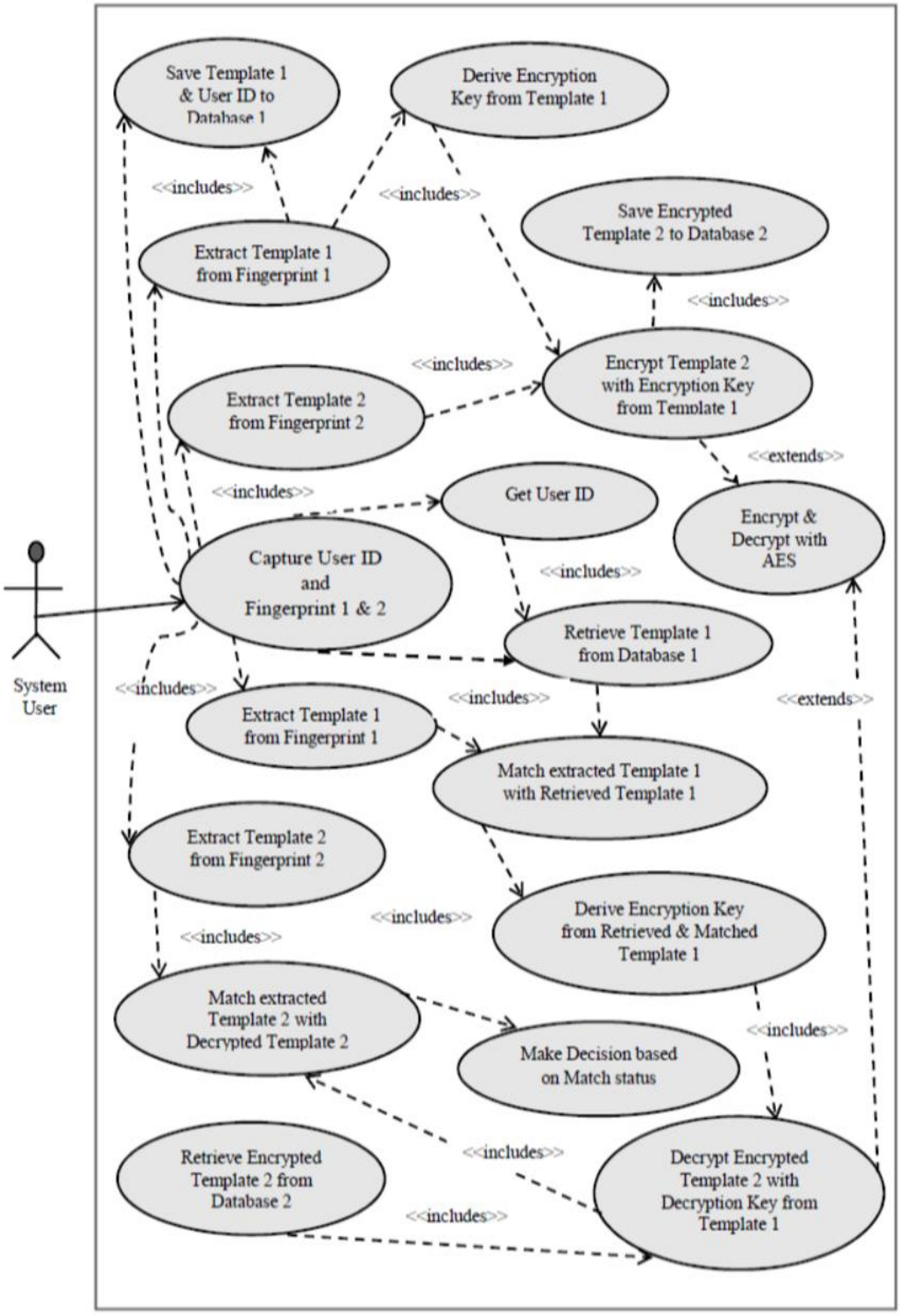
viii. System is able to capture fingerprint images and save them in desired computer folder locations.

ix. System should on refresh, clear logs, clear fingerprint image and clear minutiae data table.

4.2 Use Case Diagram

To model the dynamic nature of the two-step biometric fingerprint encryption and decryption tool, we utilized a use case diagram to model the subsystems of this tool. *Figure 2* shows the use case diagram of this system.

Figure 2. Use Case Diagram



4.3 System Implementation

4.3.1 Tools and Technologies

Java programming language was used to code the logic of the system. Netbeans 8.0 IDE was used to develop the presentation and business layer. The presentation layer largely employed use of Java's Jswing components while the business logic was implemented using object oriented concept of Java programming language. Source AFIS java framework library was used to extract, enroll and match templates captured from fingerprint images using a Digitalpersona U.are.U 4000 fingerprint reader.

4.3.2 Database and Database Tools

MySQL 5.1 database was used to create the two databases required by the two-step biometric fingerprint encryption and decryption system. HeidiSQL 8.3 database manager was employed to aid in the visual design and modelling of the table structures in the two databases.

4.3.3 System Architecture

The system was implemented using a multi-tier architecture. The system's structured architecture consisted of presentation, application and data layers. In the presentation layer, Java's JSwing framework was used to implement form components for capturing system users' particulars, capturing of fingerprints, displaying fingerprint image patterns and viewing of tabulated minutiae data. The application layer implemented the fingerprint enrollment, verification and identification functionalities. The application layer also handled the application's logic while in the data layer, the external data source for archiving and retrieval of application's data which included fingerprint templates and user details to and from the non-embedded MySQL database was built.

4.3.4 Database Design

MySQL which is a non-embedded database as well as a relational database management system was used to store biometric fingerprint templates and user details in two databases *db1* and *db2* as shown *Figure 3* below. Database *db1* stores fingerprints templates used in first (1st) step of enrollment, verification and identification from which biometric encryption and decryption keys are derived from. *Figure 4* below shows *registration_fp1* relation where this data goes into while database *db2* stores encrypted fingerprint templates and user particulars used in second (2nd) step of enrollment, verification and identification as shown in *enc_registration_fp2* relation in *Figure 5* below.

Figure 3. System Databases

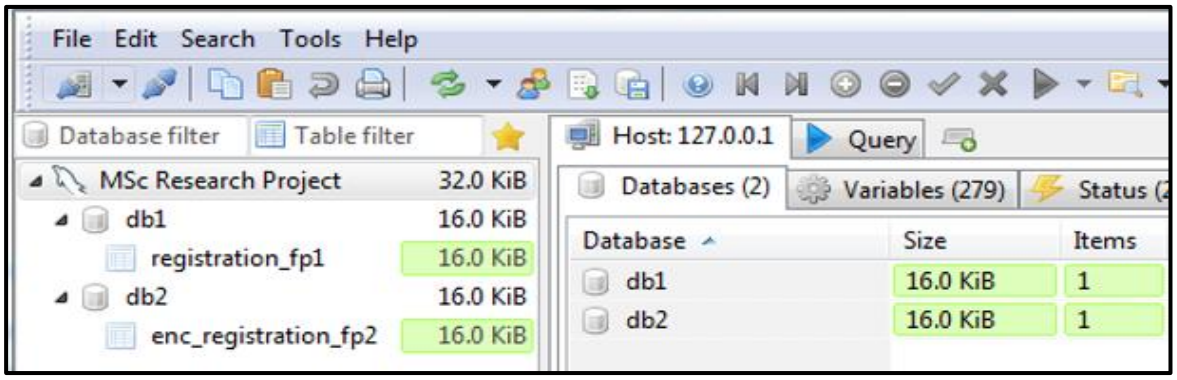


Figure 4. Registration_fp1 Table

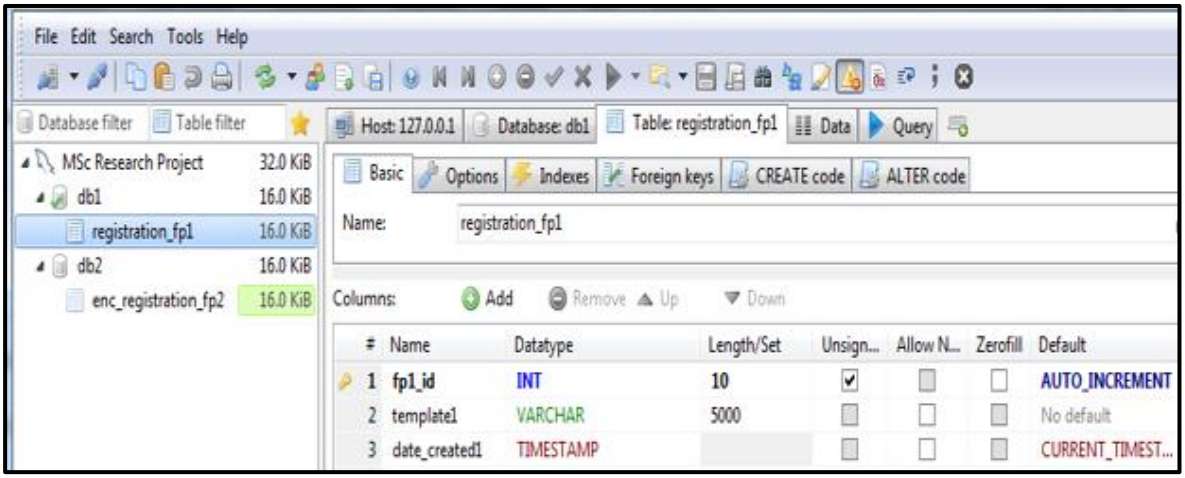
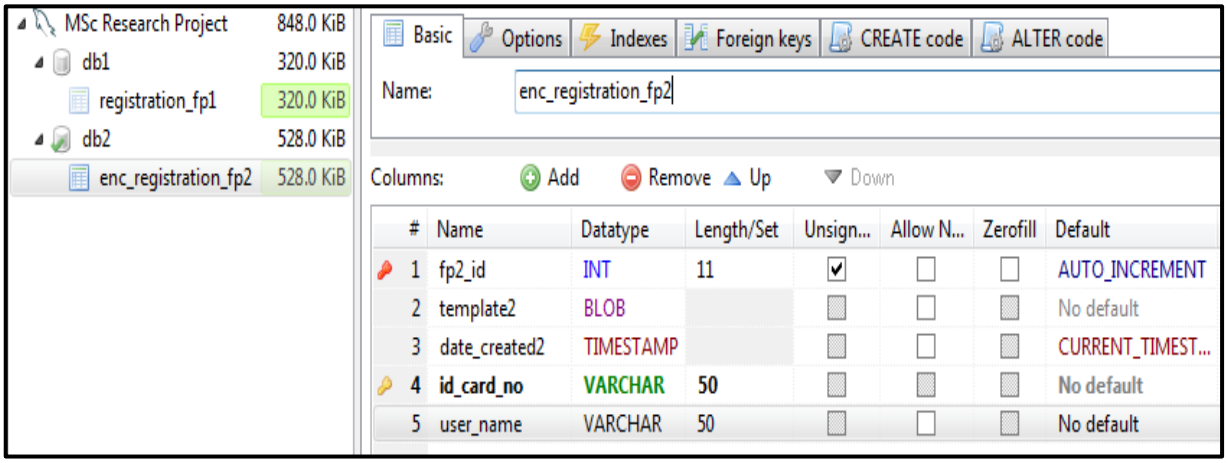


Figure 5. Enc_registration_fp2 Table



4.4 System Flow

System flow is divided into two major phases which are the two roles performed by the system. They are;

i. User Registration and Fingerprints Enrolment.
ii. User Authentication and Fingerprint Matching.

4.4.1 User Registration and Fingerprints Enrolment

System flow is divided into two major phases which are the two roles performed by the system. The following sequence of events take place in this phase. First the system prompts for user details i.e. user names and national identity card no. The system will not advance to the next steps until these details are provided. Once user particulars are supplied, system proceeds to the second step where capturing of fingerprints takes place.

Fingerprints registration process is divided into two other sub processes. The first one is where the user supplies their first fingerprint for enrolment preferably any of their index finger. The finger once captured, the system extracts a fingerprint template ***t1*** from it and then the biometric fingerprint encryption modules extract a unique biometric key ***ek*** from it. The system then prompts the user to present the second fingerprint for enrolment after which it extracts a biometric fingerprint template ***t2*** from it.

Once the user's details have been entered, fingerprints captured for enrolment and biometric encryption key ***ek*** is derived from the first enrolled fingerprint ***t1***, the system then encrypts the second user's fingerprint template ***t2*** with the encryption key ***ek*** derived from the first fingerprint template ***t1*** to encrypted template ***et2*** which is now secured. This step completes with the system saving the first fingerprint template to database ***db1*** and saving of the encrypted fingerprint template ***et2*** together with the supplied user details to database ***db2***. *Figure 6* shows a diagrammatic flow of fingerprint registration process.

4.4.2 User Authentication and Fingerprint Matching

This phase verifies and identifies system users. In ***verification*** the user is authenticated against user details they provide while in ***identification*** the user is authenticated from looping thru the entire fingerprint databases. In either verification or identification if the presented fingerprint is similar to the one saved in database ***db1*** the system alerts for fraudulent system use because due to the noisy nature of fingerprint images, no two fingerprint images from the same fingerprint should be similar to each other.

In ***verification***, system user is prompted to enter identity number. System then searches database ***db1*** for fingerprint template ***t1*** saved against the supplied identity number. If the identity number provided exists, the system retrieves fingerprint template ***t1*** saved against it in readiness for matching. The system then prompts the user to present their fingerprint for capturing of fingerprint image and extraction of template ***vit1*** to be matched against template ***t1*** in the ***1st*** first step of ***verification***. If presented fingerprint does not match the verification process ends but if the presented fingerprint and template t1 match the system proceeds to the 2nd step of verification.

In the ***2nd*** second step of ***verification***, the system prompts the user to present the second fingerprint for capturing and extraction of fingerprint template ***vit2*** for verification. The system then derives decryption key ***dk*** from matched template ***t1*** in first step of verification. The decryption key ***dk*** attempts to decrypt templates in database ***db2*** by looping thru all templates in database ***db2***. If an encrypted template ***et2*** is successfully decrypted to ***dt2***, the template is matched against template ***vit2*** extracted from the second fingerprint presented for verification. When the two templates ***dt2*** and ***vit2*** match, the system returns and displays the user details i.e. their names and identity number but if the two templates do not match the verification process ends and returns notification that there was no match.

In ***identification***, system prompts user to present their fingerprint for capturing of fingerprint image and extraction of template ***vit1*** to be matched against looping of templates ***t1*** in database ***db1*** in the ***1st*** first step of identification. If presented fingerprint does not match with any of the templates in database ***db1*** the identification process ends but if the presented fingerprint and and a template ***t1*** match the system proceeds to the 2nd step of identification.

In the ***2nd*** second step of ***identification***, the system prompts the user to present the second fingerprint for capturing and extraction of fingerprint template ***vit2*** for identification. The system then derives decryption key ***dk*** from matched template ***t1*** in first step of identification. The decryption key ***dk*** attempts to decrypt templates in database ***db2*** by looping thru

all templates in database ***db2***. If an encrypted template ***et2*** is successfully decrypted to ***dt2***, the template is matched against template ***vit2*** extracted from the second fingerprint presented for identification. When the two templates ***dt2*** and ***vit2*** match, the system returns and displays the user details i.e. their names and identity number but if the two templates do not match the verification process ends and returns notification that there was no match. *Figure 7* shows a diagrammatic flow of both fingerprint verification and identification process.

Figure 6. User Registration and Fingerprints Enrolment

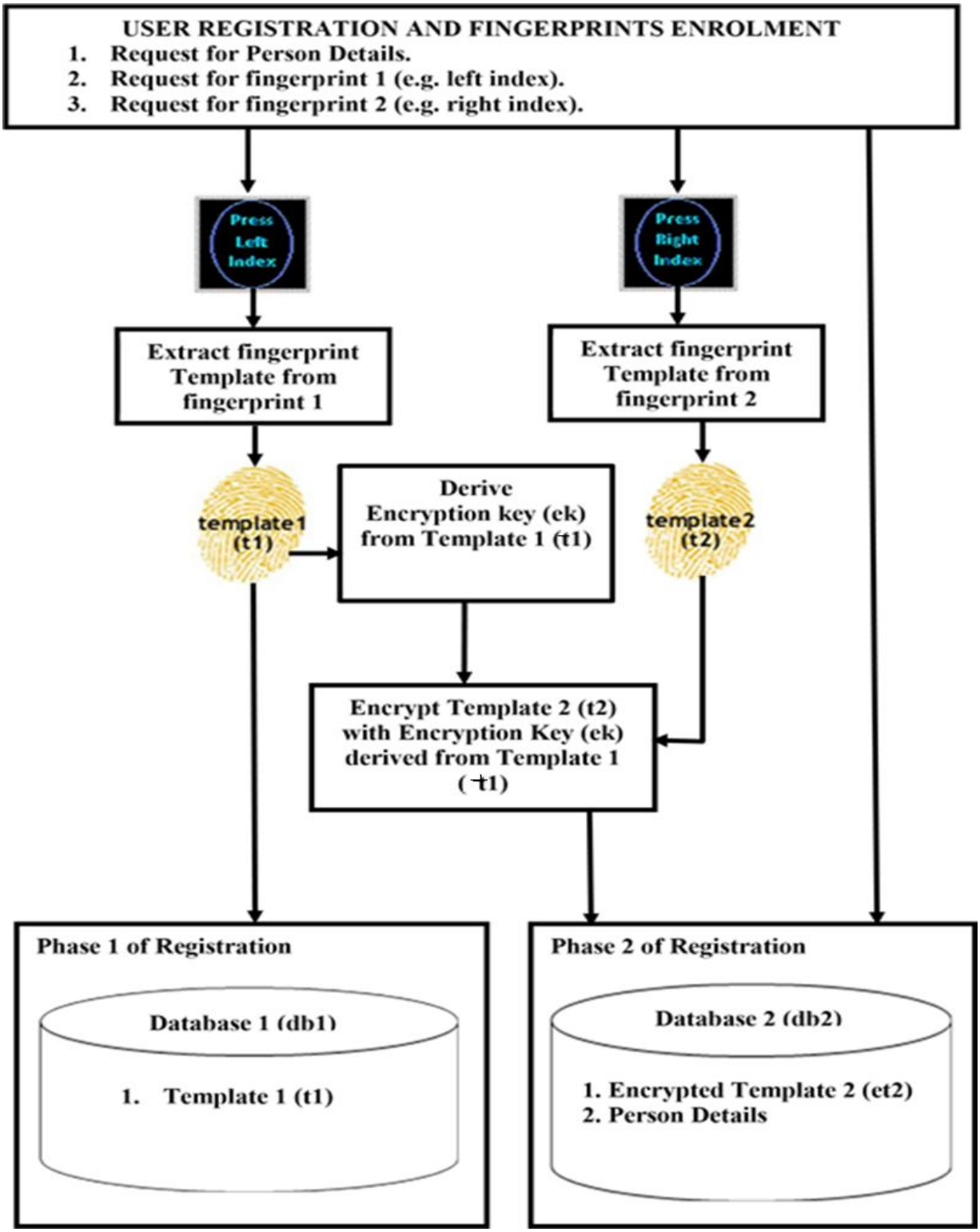
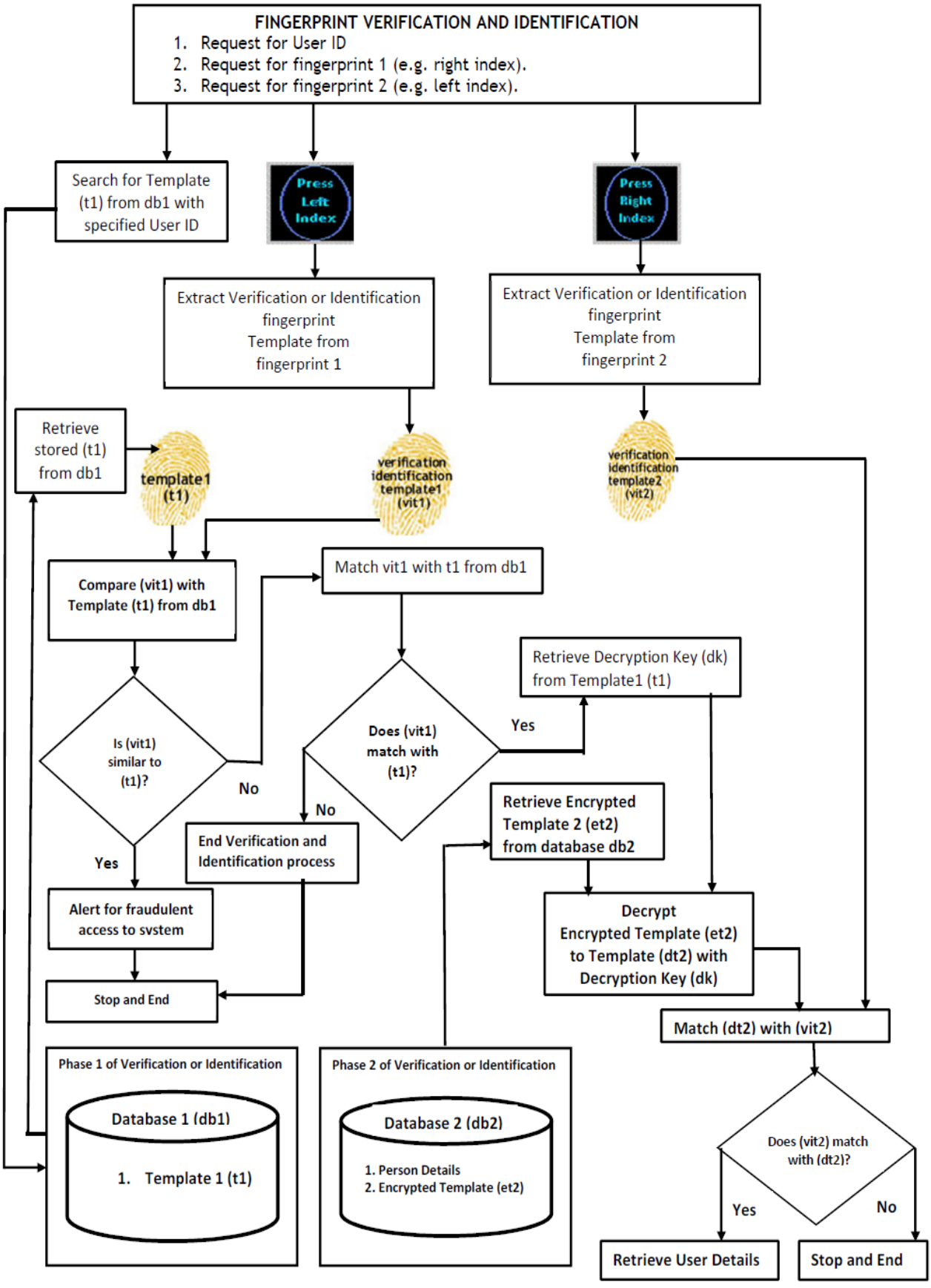


Figure 7. Fingerprint Verification and Identification



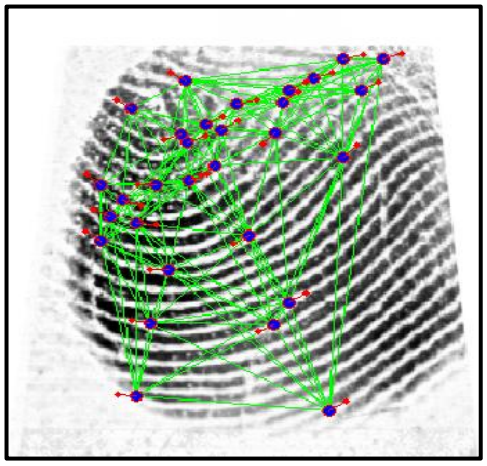
4.5 System Graphical User Interface

The system's user interface consisted of the following; fingerprint view panel, system logs panel and the fingerprint minutiae data table.

4.5.1 Fingerprint View Panel

When a fingerprint is presented on a fingerprint reader, the captured fingerprint image is displayed on the system's fingerprint view panel. The fingerprint view panel shows ridges i.e. bifurcations and ridge endings patterns on a fingerprint image which are the physiological patterns that uniquely identify a person from another. *Figure 8* shows physiological patterns captured and displayed on a fingerprint view panel.

Figure 8. Fingerprint View Panel



4.5.2 System Logs Panel

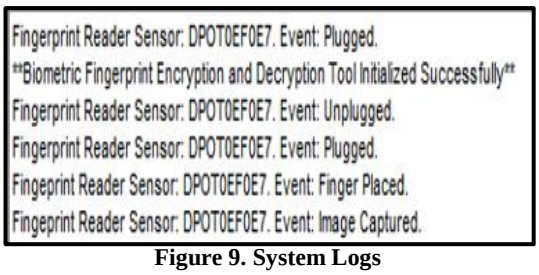


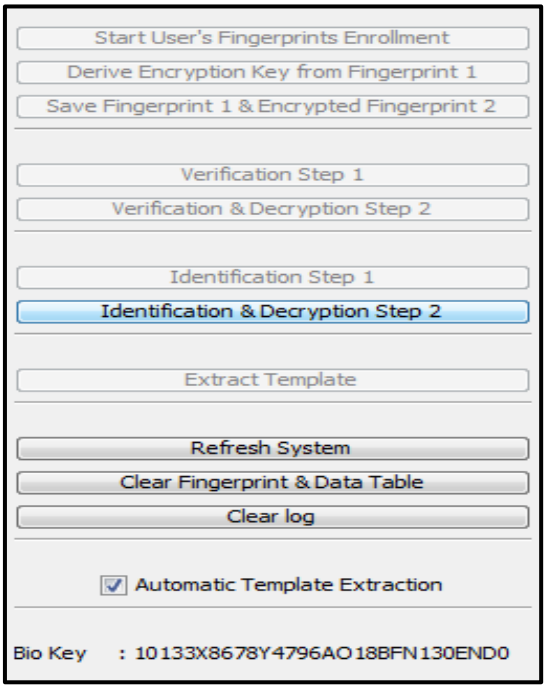
Figure 9. System Logs

The logs of events and activities taking place in the system are logged at the system logs panel. A system user is notified of events such as successful system initialization, plugged in fingerprint reader, unplugged fingerprint reader and captured fingerprint image form the system logs panel. *Figure 9* shows tracked events logged in system logs panel.

4.5.3 System Buttons Panel

Buttons which are used to do the main functions of the system i.e. fingerprints enrollment, user verification and user identification are docked in the system buttons panel. System buttons panel is also used to hold refresh button which resets the whole system, clear log button which cleans all displayed system logs and the 'clear fingerprint and data table' button which clears fingerprint view panel and fingerprint minutiae data table panel. This panel is also used to display the biometric key label which outputs the derived biometric key and auto extract check box which is used to prompt the system to perform automatic fingerprint template extraction. System buttons panel is shown in *Figure 10* below.

Figure 10. System Buttons Panel



4.5.4 Fingerprint Minutiae Data Table Panel

The fingerprint minutiae data table panel displays minutiae data of templates extracted from fingerprint images. It is refreshed and repopulated again with minutiae data of a fingerprint image every time a fingerprint image is captured form the fingerprint reader sensor module. Minutiae column shows the number of minutia, ***X*** column shows the minutia's position on the ***x***-axis, ***Y*** column shows the minutia's position on the ***y***-axis, ***DIRECTION*** column show the minutia's angle of orientation given its ***x*** and ***y*** coordinates and ***RIDGE TYPE*** column determines whether the ridge type is a bifurcation or an ending. *Figure 11* shows minutiae data extracted from a template and exhibited in a fingerprint minutiae data table panel.

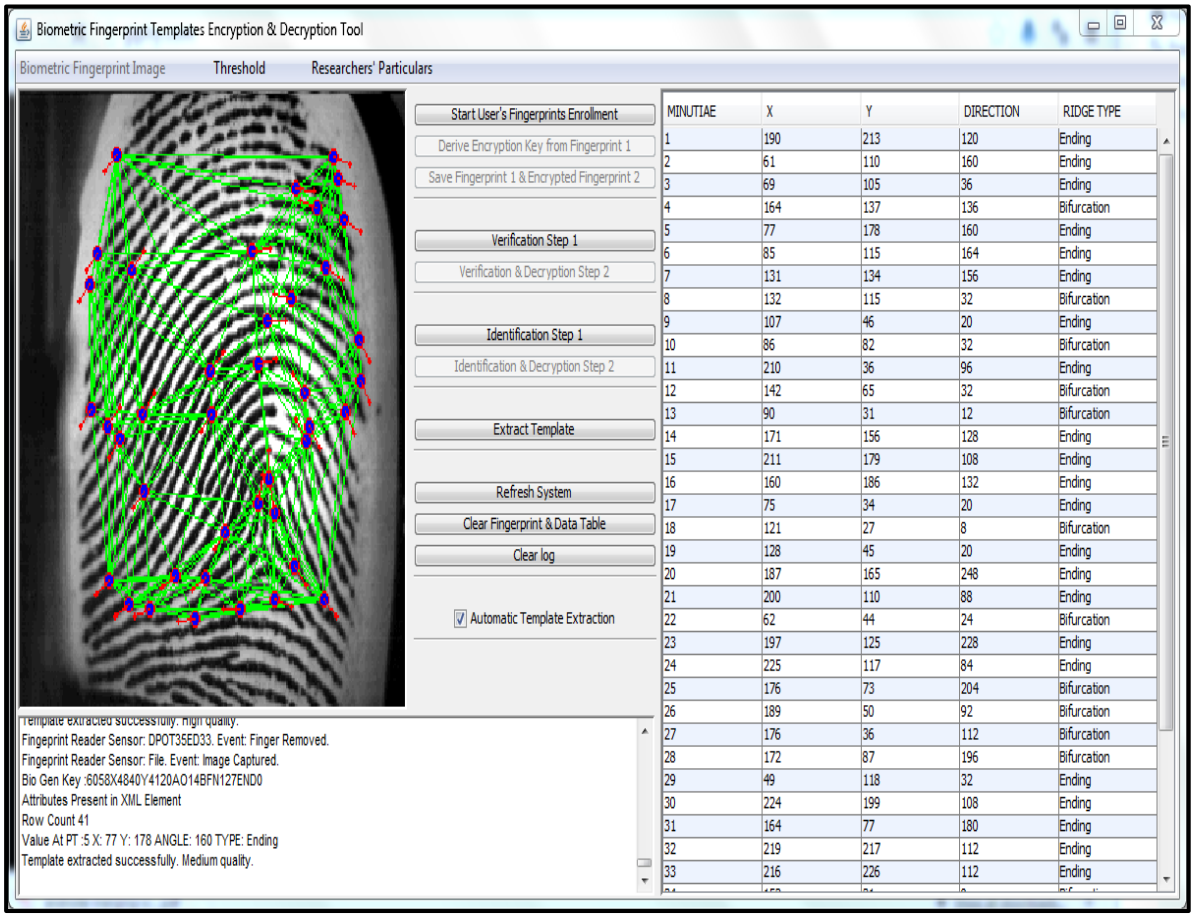
4.5.5 System's Main GUI

The form in which the user interacts with the system is the system's main form. It has on its menu bar the following items; a provision for loading and saving fingerprint images and a provision for viewing researchers' particulars. *Figure 12* below shows the system's main frame which anchors the fingerprint view panel, system logs panel, system buttons panel and the fingerprint minutiae data table panel.

Figure 11. Fingerprint Minutiae Data Table

MINUTIAE	X	Y	DIRECTION	RIDGE TYPE
1	115	235	112	Bifurcation
2	258	266	160	Ending
3	197	209	24	Ending
4	133	145	248	Ending
5	223	160	152	Ending
6	124	218	120	Bifurcation
7	213	144	20	Ending
8	145	184	0	Ending
9	214	284	32	Bifurcation
10	270	315	148	Ending
11	137	246	0	Bifurcation
12	158	249	144	Bifurcation
13	121	302	236	Ending
14	107	223	240	Bifurcation
15	175	260	28	Bifurcation
16	179	286	152	Ending
17	239	324	140	Ending
18	189	305	136	Ending
19	219	306	156	Ending
20	284	338	140	Bifurcation
21	223	315	148	Ending
22	258	338	136	Ending
23	101	246	228	Bifurcation
24	157	277	144	Ending
25	153	283	16	Ending
26	101	205	232	Ending
27	169	290	148	Ending
28	156	322	236	Bifurcation
29	124	92	252	Ending
30	249	81	152	Ending

Figure 12. System's Main GUI



5. TEST RESULTS

5.1 Test Description and Introduction

In testing of the developed biometric fingerprint encryption and decryption tool, 600 fingerprint templates were extracted, enrolled and saved to the system's database. Portions of the research in this paper use the CASIA-FingerprintV5 collected by the Chinese Academy of Sciences' Institute of Automation (CASIA) [14]. The fingerprint images were captured using Digitalpersona 4000 U.are.U fingerprint readers.

Fingerprint images used during test were majorly categorized into two (2) i.e. fingerprints used to derive encryption keys in the 1st step of enrollment and authentication. The other category of fingerprints were used in 2nd step of enrollment and authentication where they were encrypted before being saved to database and decrypted before authentication of fingerprints. Out of the 600 fingerprint images used, 300 were used to derive encryption keys and this study derived encryption keys from fingerprints of the left hand and used them to encrypt fingerprints from the right hand. Table 1 shows this data where out of each of the three fingers types used from each hand i.e. thumb, index and middle fingers, each finger type had one pair from which an encryption key was derived in 1st step of enrollment then used to encrypt the other pair in 2nd step of enrollment.

Table 1. Overall Test Results for Pass and Fail during Decryption in 2nd step of Verification and Identification

LEFT HAND FINGERPRINTS WHICH WERE USED IN 1ST STEP OF AUTHENTICATION AND TO DERIVE ENCRYPTION KEYS			RIGHT HAND FINGERPRINTS WHICH WERE ENCRYPTED AND USED IN 2ND STEP OF AUTHENTICATION		
RIGHT HAND FINGER TYPE	TOTAL FINGER TYPE COUNT	TOTAL COUNT OF RIGHT HAND FINGERPRINT TEMPLATES USED	LEFT HAND FINGER TYPE	TOTAL FINGER TYPE COUNT	TOTAL COUNT OF LEFT HAND FINGERPRINT TEMPLATES USED
THUMB	100	300	THUMB	100	300
INDEX	100		INDEX	100	
MIDDLE	100		MIDDLE	100	

Table 2. Overall Test Results for Pass and Fail during Decryption in 2nd step of Verification and Identification

VERIFICATION AND IDENTIFICATION STATUS AFTER DECRYPTION OF LEFT FINGERPRINT TEMPLATES	COUNT	PERCENTAGE
PASS	181	60.33%
FAIL	119	39.67%
ALL STATUS COUNTS	**300**	**100%**

Table 3. Statistics of Finger Types used to Test for Decryption in 2nd step of Verification and Identification

FINGER TYPE USED FOR VERIFICATION AND IDENTIFICATION OF DECRYPTED LEFT FINGERPRINT TEMPLATES	TOTAL LEFT FINGER TYPE COUNT
THUMB FINGERS	100
INDEX FINGERS	100
MIDDLE FINGERS	100
TOTAL FINGERS DECRYPTED	300

5.2 Overall Test Results

From the test results carried out, 181 (60.33%) of fingerprints templates in 2nd step of verification and identification were decrypted successfully and matched to their corresponding fingerprint type. 119 (39.67%) of fingerprints did not pass the decryption test. These results are shown in Table 2.

Table 4. Test Results for all the Finger Types used in Encryption and Decryption at 2nd step of verification and Identification

FINGER TYPE	VERIFICATION AND IDENTIFICATION STATUS AFTER DECRYPTION OF LEFT FINGERPRINT TEMPLATES	STATUS COUNT PER LEFT FINGER TYPE	OVERALL LEFT FINGER TYPE COUNT	STATUS PERCENTAGE PER LEFT FINGER TYPE
THUMB	PASS	63	100	63%
	FAIL	37		37%
INDEX	PASS	60	100	60%
	FAIL	40		40%
MIDDLE	PASS	58	100	58%
	FAIL	42		42%

5.3 Finger Type allocations for Test of Decryption before Verification and Identification

Three fingerprint types were used to carry out tests. They were the thumb, index and middle finger. From each finger type, 100 fingerprint images from 100 persons were used to test the decryption capability of the developed system such that the total number of fingerprint images encrypted and tested during decryption and authentication step were all together 300 fingerprint images. Table 3 represents these allocations per finger type as shown below.

5.4 Respective Finger Type Results during Verification and Identification after Decryption

From the finger types used, verification and identification results after decryption of fingerprint templates in 2nd step of authentication showed that 63 (63%) of Thumb fingerprint templates were decrypted and authenticated successfully while 37 (37%) could not be verified or identified after decryption. 60 (60%) of Index fingerprint templates were decrypted and authenticated successfully while 40(40%) could not be verified or identified after decryption and last 58(58%) of middle fingerprint templates authenticated successfully while 42(42%) could not be verified or identified after decryption. These results are represented in Table 4.

5.5 Test Results Analysis and Summary.

The biometric fingerprint encryption and decryption tool demonstrated encryption and decryption of fingerprint templates in a unimodal biometric system utilizing encryption keys derived from other biometric fingerprint templates as a robust technique of securing biometric fingerprint templates in database. Results from tests carried out attested it is a viable approach towards alleviating type 6 attacks on biometric systems which is the attack of biometric templates in a biometric system's database.

Test results showed that 63 (63%) of thumb, 60(60%) of index and 58 (58%) of middle fingerprint templates could be decrypted and authenticated with the corresponding finger type but 37 (37%) of thumb, 40 (40%) of index and 42 (42%) of middle fingerprint templates could not be authenticated after decryption. To understand this discrepancy, the particular fingerprint that failed the tests were critically observed and analyzed. It was ascertained that some of these fingerprint images did not have elaborate physical feature traits. This can be attributed to the bearer's fingerprints being scratched and bruised from doing hefty menial jobs. Another factor that could have contributed to this is the inability of fingerprint sensor used to be able capture clear fingerprint images from sweaty and dry hands. The other likelihood cause of low quality images that did not pass decryption and authentication step could possibly have been paramount intra-class variations of fingerprint images resulting from the sundry levels of pressure and rotation of fingerprints on the fingerprint reader by the volunteers who donated fingerprint.

Test results with positive status outcomes after decryption and authentication of fingerprints can be ameliorated by utilizing advanced fingerprint readers like laser based finger sensors which can capture clear fingerprint images despite the known subsisting caveats that impede efficient extraction of fingerprint templates from fingerprint images. To reduce capture of low quality fingerprint images from sweaty and dry fingerprints, the following two practices can be put into practice. Persons with sweaty and wet fingers could be asked to dry their fingerprints on a piece of cloth afore presenting them on a fingerprint reader sensor e.g. rub their fingers on their attire while persons with dry fingers could be requested to rub their fingers on their face to make them moist. Washing of hands and oiling them could additionally avail in reducing capture of low quality fingerprint images.

6. CONCLUSION

The main purport of this study was to establish a more secure and efficacious technique for securing biometric fingerprint templates stored in a database that would be predicated on encryption keys derived from other biometric fingerprint templates. To accomplish this objective, it was essential to ascertain the sundry biometric attacks and threats acknowledged in subsisting literature. Thereafter the biometric template protection schemes and techniques currently being used towards securing biometric templates against biometric systems' database attacks were explored and analyzed. In the end, a biometric fingerprint encryption and decryption software tool that could derive encryption and decryption keys from biometric fingerprint templates was built. In our proposed biometric templates encryption and decryption tool, encryption and decryption keys have to be derived from biometric fingerprint templates in order to be used. This tool achieved a secure way of obscuring encryption keys in biometric templates away from hackers prying eyes and would be adversarial attacks determinedly targeting to access biometric decryption keys in a unimodal biometric system. Future research directions will require researchers to

study ways of deriving encryption keys from fingerprints that will engender encryption keys which do not vary with reiterated fingerprint image scans due to the noisy nature of fingerprint images and at the same time obviate generation of encryption keys that would be facile to attack by utilization of brute force.

7. REFERENCES

[1] Das, A. K. (2011, March). Cryptanalysis and Further Improvement Of a Biometric-Based Remote User Authentication Scheme Using Smart Cards. *International Journal of Network Security & Its Applications (IJNSA), 3*(2), 13-28.

[2] Mwema, J., Kimani, S., & Kimwele, M. (2015, February). 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), 108-119.

[3] Das, R. (2012, February). Multimodal biometric systems How they can help to protect against physical and logical threats. *Keesing Journal of Documents & Identity*(37).

[4] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*.

[5] Du, E. Y., Yang, K., & Zhou, Z. (2011, October). Key Incorporation Scheme for Cancelable Biometrics. *Journal of Information Security*, 185-194.

[6] Das, P., Karthik, K., & Garai, B. C. (2012, September). A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition, 45*(9), 3373-3388.

[7] Gaddam, S. V., & Lal, M. (2011). Development of Bio-Crypto Key From Fingerprints Using Cancelable Templates. *International Journal of Academic Excellence in Computer Applications, 4*(8), 137-145.

[8] Blanton, M., & Aliasgari, M. (2013). Analysis of Reusability of Secure Sketches and Fuzzy Extractors. *Journal of Computer and System Sciences, 58*, 148-173.

[9] Hooda, R., & Gupta, S. (2013, April). Fingerprint Fuzzy Vault: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(4), 479-482.

[10] Al-Saggaf, A. A., & Acharya, H. (2013). Statistical Hiding Fuzzy Commitment Scheme for Securing Biometric Templates. *International Journal of Computer Network and Information Security*, 8-16.

[11] Maniroja, M., & Sawarkar, S. (2013). Biometric Database Protection using Public Key Cryptography. *IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.5, May 2013.*

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

[13] Mwema, J., Kimani, S., & Kimwele, M. (2015, February). 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.

[14] *CASIA-FingerprintV5*, http://biometrics.idealtest.org/

[15] Bansal, R., Sehgal, P., & Bedi, P. (2011, September). Minutiae Extraction from Fingerprint Images. *International Journal of Computer Science Issues, 8*(5), 74-85.

[16] Alanazi, H., Zaidan, B., Zaidan, A., Jalab, H., Shabbir, M., & Al-Nabhani, Y. (2010, March). New Comparative Study Between DES, 3DES and AES within Nine Factors. *Journal of Computing, 2*(3), 152-157.