American Journal of Bioinformatics Research 2016, 6(3): 99-112
DOI: 10.5923/j.bioinformatics.20160603.01

Development of Fingerprint Biometrics Verification and Vetting Management System

Joseph Kalunga*, Simon Tembo

Department of Electrical and Electronic, School of Engineering, University of Zambia, Lusaka, Zambia

Abstract This paper presents the development of fingerprint biometrics verification and vetting management system for Sensitive Organization. The idea behind this study is to improve security in sensitive institutions through integration of fingerprint biometrics into identity database. A fingerprint is a very recognized and acceptable security feature. It is traditionally used for human identification and criminal vetting of newly recruited security staff. There was need to develop Human Identity Authentication System that verify the true identity of people gaining entry into sensitive institution as an additional security layer to existing traditional techniques (National Identification Card, Driving license and passport). Traditional Techniques of human identity verification suffer from security Vulnerabilities such as masquerading identity; mobility issues (include lost, forgery and misplacement) and inaccuracy. The study was conducted using visual studio 2010 on DotNet framework 4.0 with C# object oriented programming language. The backend database used was MySQL relational database management system (RDMBS). The research produced a number of key results include the development of biometric security layer that is able to identify and verify identity of an individual using enrolled fingerprint template. Other results include the ability to capture military police security data, storage, retrieval and dissemination. The developed application performance was evaluated by enrolled ten fingerprints and captured related individual personal information. The result indicated 99.999% biometric accuracy levels attained with error allowance of 0.001% False Acceptance Rate (FAR) and 0.001% False Rejection Rate (FRR). In conclusion, the study shows that the integration of fingerprint biometric system in sensitive institution database can improve security of the organization and alleviate problem associated with traditional identity verification techniques.

Keywords Fingerprint, Biometric System, Identity, Vetting, Verification, Database

1. Introduction

The true identity of a person visiting a sensitive institution can accurately be verified using combination of secret key and biometric system. Secret key identity verification methods refer to the usage of traditional techniques of human identity recognition. While a Biometrics is an automated method of recognizing a person based on a biological or behavioural characteristic [1]. Among the features measured are face, palms, DNA, body orientation in motion, fingerprints, hand geometry, handwriting, iris, retinal, vein, signature and gait. The term biometrics is derived from the Greek words bios (meaning life) and metron (meaning measurement) [2]. Biometrics technologies measure and analyse living human body characteristics for authentication, verification and identification purposes. Any human physiology, chemistry or behaviour can be used as biometric identifier. However biometric identifier must poses attributes such as Universality, Uniqueness, Permanence, Measurability, Performance, acceptability and Circumvention [3].

Traditional approach of human identity verification is currently practiced in developing countries to secure installations of strategic importance such as military installations. It involves an employment of National Identification Card, driving licence or travelling passport to identify the real identity of the guest. This approach has security concerns include impersonation and masquerading of identity [3]. This concern is possibly alleviated by biometric solution. Biometric solutions require enrolment process, input of biographic data and storage of these identity parameters in the database. This principle is applicable to all biometric systems. However, fingerprint biometrics is more accurate, unique, immutability and acceptable than any other biometrics system [4]. Because of the versatility of fingerprint in the military, we have developed an application that augments security aspects.

2. Related Works

In 1998, Gorman [5] described fingerprint verification

* Corresponding author:
josephkalunga@yahoo.com (Joseph Kalunga)
Published online at http://journal.sapub.org/bioinformatics

methods and technologies. Its purpose was to give an understanding on fingerprint verification, recognition and system design considerations. His study also gave an impression on fingerprint technologies, its advantages and disadvantages in reference to other biometrics systems.

In [6] 2010, The US and UK developed biometrics systems to identify non-authorized personnel. The system compared details captured and stored in database through intelligent means with live details submitted by visitors. The system received a lot of praises because it was able to identify an individual and cross-matching the biometric data to their own databases in the quickest possible time. This resulted in the US department for Home Land Security to introduce a pilot program 'fidge factor'. Fidge factor is the behavior biometrics system to determine whether or not interviewees were hostile to the US.

In [6] the same year 2010, the afghan government developed Afghan Automated Biometrics Identification system (AABIS). In this system fingerprints, iris and face were scanned and stored in the database. The system was developed to enhance security in the nation. This system produced among other documents a smart card Identification Card (ID) to identify afghan citizen.

In [7] 2011, UK developed surveillance and identity management system. The system was developed to issue UK Biometrics Resident Permit to foreign nationals includes visiting scholars, entrepreneurs, professional, investors and domestic workers. The system had three important modules namely; enrollment, surveillance and personal identity.

In [4] 2013, Countries around the world employed biometric systems at the border. The said biometric system seeks to tighten up security at borders. We propose the Development of fingerprint biometrics verification and vetting management system to secure sensitive organization.

In [8] 2014, Adewale proposed the development of fingerprint biometrics attendance systems for non- academic staff in tertially institution. The system was developed to manage attendance record in an organization using the available computer development tools. The proposed application captures attendance electronically with the help of fingerprint recognition system. In Adawawe's work the emphasis was to reduce labour intensiveness associated with manual attendance record system.

3. Materials and Methodology

The materials used in this study are divided in to two categories hardware and software. A hardware material refers to tangible equipment used in the study such as Personal Computer (PC), fingerprint optic scanner and digital camera. Software materials denote substances that could not be seen or touched. They are virtual objects and were used in application development. Software tools include visual studio 2010, WAMP Server version 2.2, and fingerprint scanner System Development Kit (SDK) version 5.0. In terms of Software development methodology, the study adopted agile software development methodology. The hardware tools and their specification are tabulated in table 1.

Table 1. Hardware tools and Specifications

Hardware	Specification
PC	- Hard disk 80GB Minimum - Processor 3.2 GHz Minimum. Preferable core i3 and above - RAM 4.0 GB - Graphics frequency 3.30 MHz - 64-bit Operating System
Fingerprint Scanner	- Image resolution 500 pixels per inch. - Image area 9.75mm X 0.41mm/ 192 X 8 pixel - ISO / IEC 7816 T=0 and T=1 - Up to 8Mhz smart cards, and a 412 Kbit/s communication speed
Digital Camera	- 18.0 Megapixels - 18-55mm lenses - Speed 3frs - Full-high definition

4. Application Modeling

Use case diagram was used as the first step in system process modelling and this process is referred to as data diagramming. The Use Case diagram is an UML design tool and is used to visualize the behaviors of the proposed system. These include description of expected users and their system interaction levels that ultimately specify system requirements. System requirements in software engineering composed of system users, activities, their associations, dependencies, roles, processes and goals. The developed application model consists of the following modules: 1) Personal Identity Verification, 2) Fingerprint enrolment, 3) Identification, 4) Criminal Vetting, 5) Criminal Investigation, 6) Fingerprint Donor, 7) Forensic Investigation, and 8) Fingerprint Analysis as shown in figure 1.

5. System Activities

System activities are divided in two sections. The first section deals with human identity authentication. It is normally deployed at the entry point as an access control mechanism. While the second module covers security duties. Security section involves keeping the crime record, issuing identity cards, conducting criminal vetting of newly recruited soldiers and army officers. The vetting process is extended to civilian government workers deployed to work in sensitive institutions. Domestic workers who are working at officers and security married quarters are also vetted security wise.

5.1. Identity Authentication

The developed fingerprint biometrics verification and vetting management system consists of series of activities. Firstly, guests visiting military camp must identify themselves before military police officers guarding the main gate or entry points. This is normally done verbally and approaching guest must stand still at least 10 meters away from an officer for security reason. The officer on guard orders the visitor to advance some paces forward with his hands up. The guest is flicked to detect the possession of dangerous weapons (gun, knife, bombs and others). If the visitor is cleared of that check, he then avails identity documents. The officer on duty in turn verifies visitor identity through checking details appearing on guest National Identification Card or passport. After That the Computer Biometric System is request for intelligence about the visitor. If the retrieved intelligence is malicious, the guest is deterred or an arrested (as terrorist or criminal) otherwise safe heaven is provided. If the search has not find any record and the guest is not on wanted list. The visitor identity details are captured including fingerprint biometrics verification bio-data (enrolment).

5.2. Biographic Record

Security officers are responsible for general security of the sensitive installations. Additionally, they do keep biographic details and statistics of service personnel, offence committed and other sensitive security information of security interest. Security officers are also responsible for issuing of service identification card and conducting security vetting of new employees. Figure 2 shows activity diagram of the proposed system.

6. Architectural Design

The architectural design of the developed integrated biometric application has three important components namely fingerprint scanner, business logic and relational database. These components were broken down further into specialised sub components such as device drivers, middleware and API. Device drivers define operating parameters of fingerprint scanner and digital camera. Each device connected to the computer system has its own driver that administers its operations. Middleware application acted has an adapter between two applications MySQL and Visual Studio 2010 [9]. The Architectural design of fingerprint biometrics verification and vetting management system is shown in figure 3.

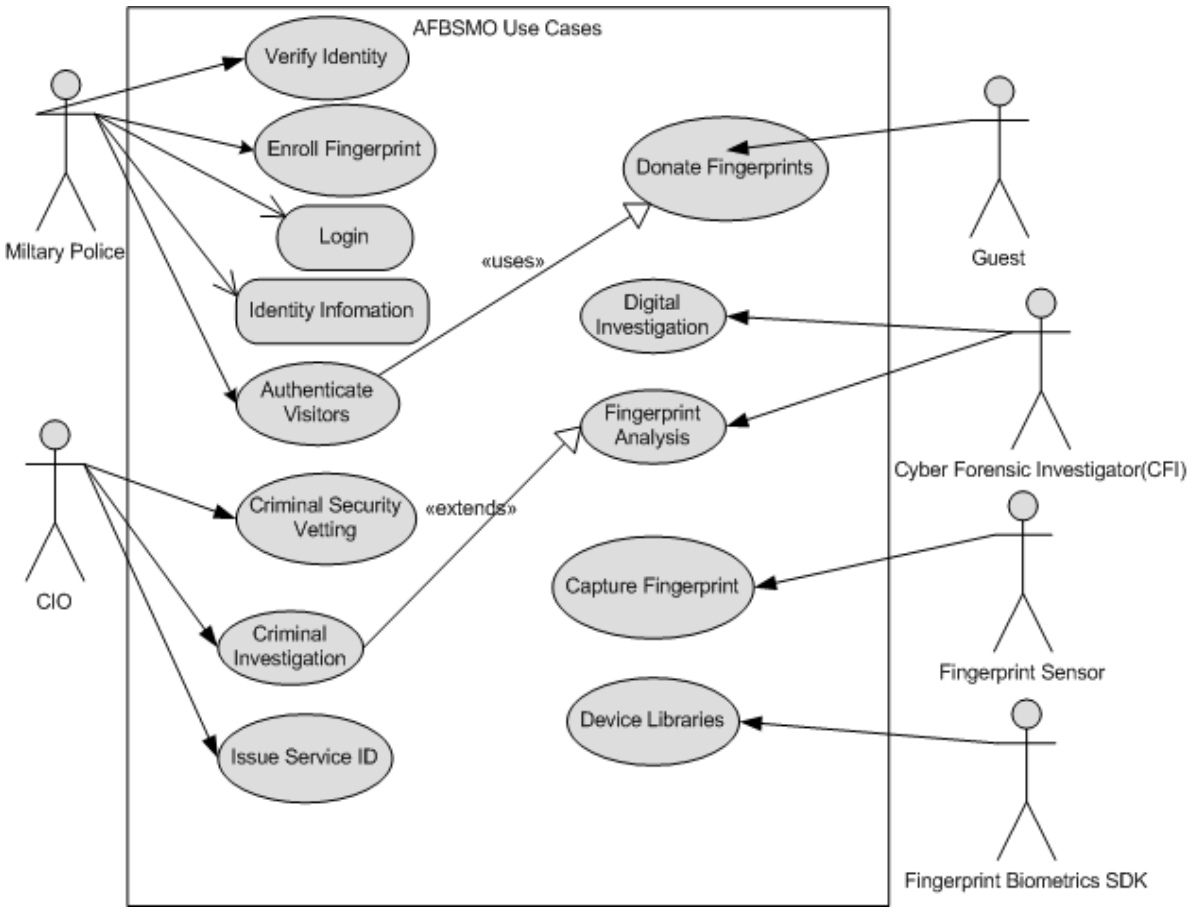


Figure 1. Use Case Diagram for Fingerprint Biometrics Verification and Vetting Management system

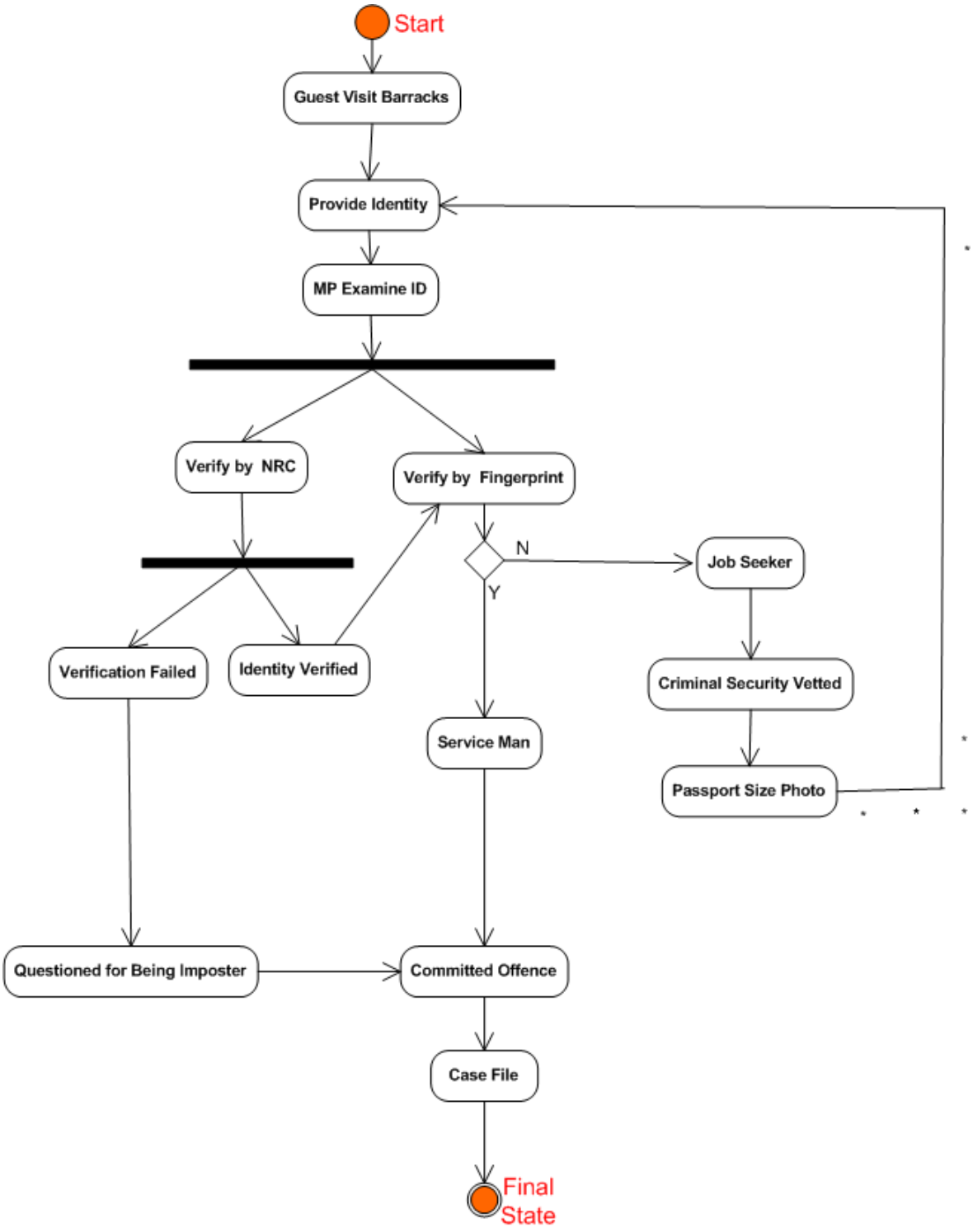
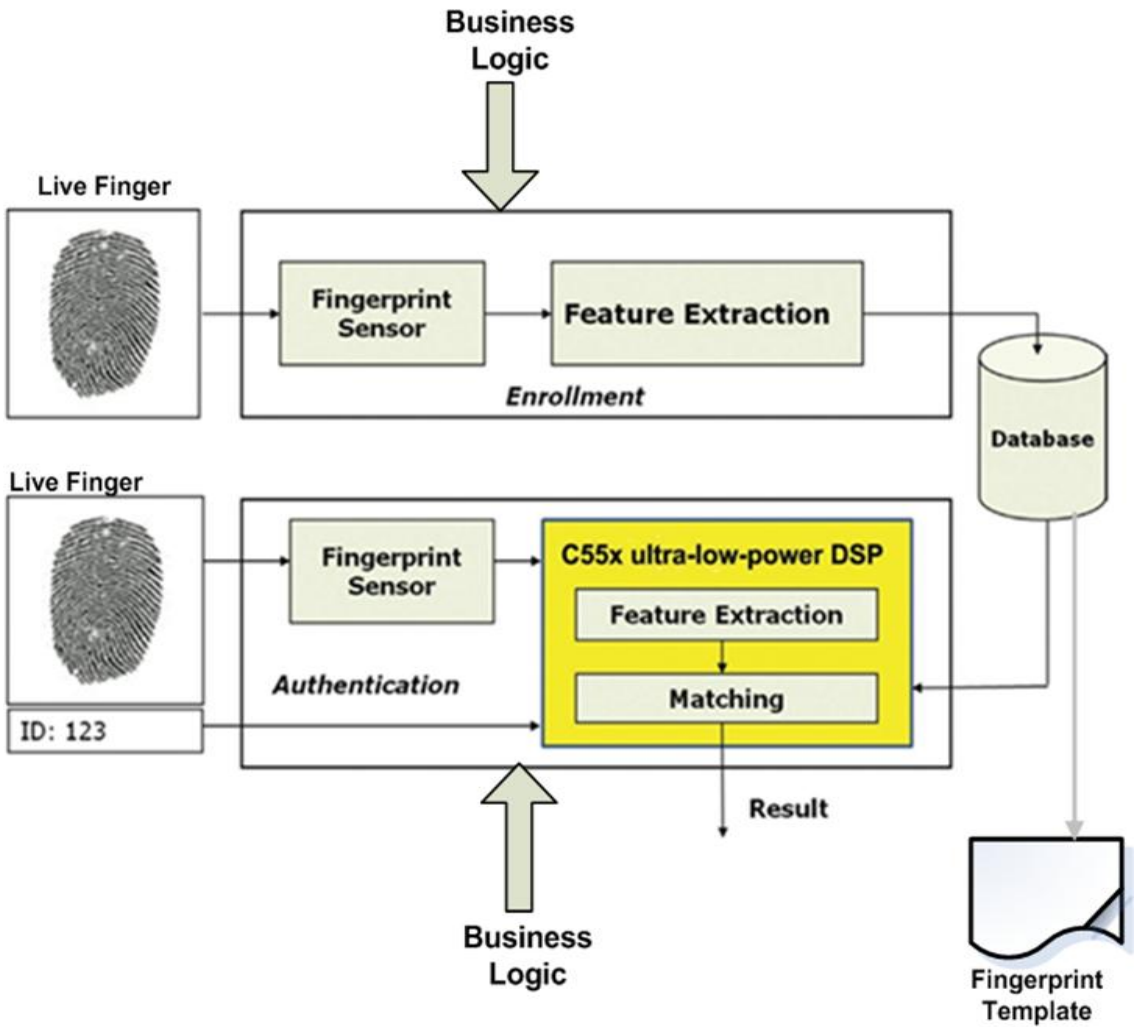


Figure 2. Activity diagram Automated Fingerprint for Military Organisation



Source: Edited [10]

Figure 3. Architectural Design for fingerprint biometrics verification and vetting management system

7. Design Components

An integrated design component contains fingerprint scanner, user interfaces and relational database. User Interfaces are divided further into data input forms and codes. The backend database design was implemented using MySQL relational database. The program was coded in CSharp(c#) object oriented programming language.

7.1. Fingerprint Scanner

Fingerprint scanner is an Optical electronic device used to capture fingerprint image from a live human finger. The research utilized U 4500 Reader scanning technology for its superior image quality and product reliability. This is because minutiae based fingerprint biometric system require high quality fingerprint image [10].

7.2. Business Logic

Business logic encompasses algorithms that encode real-world problem in to determining how data can be created, extracted, displayed, stored, and changed. Additionally, business logic describes set of rules that control some action.

7.3. Fingerprint Processing

The fingerprints captured for biometric use require further processing. This is not the case with those fingerprint capture for security vetting process which does not any process but saved directly into relational database together with personal details. Security vetting process requires the total in biometric system, input fingerprint image is processed to skeleton image levels and then features are extracted from the said thinned image. Biometrics fingerprint image processing (Digital image processing) stages includes fingerprint capturing, normalisation, segmentation, enhancement, thinning and minutiae extraction as shown in figure 4 [11].

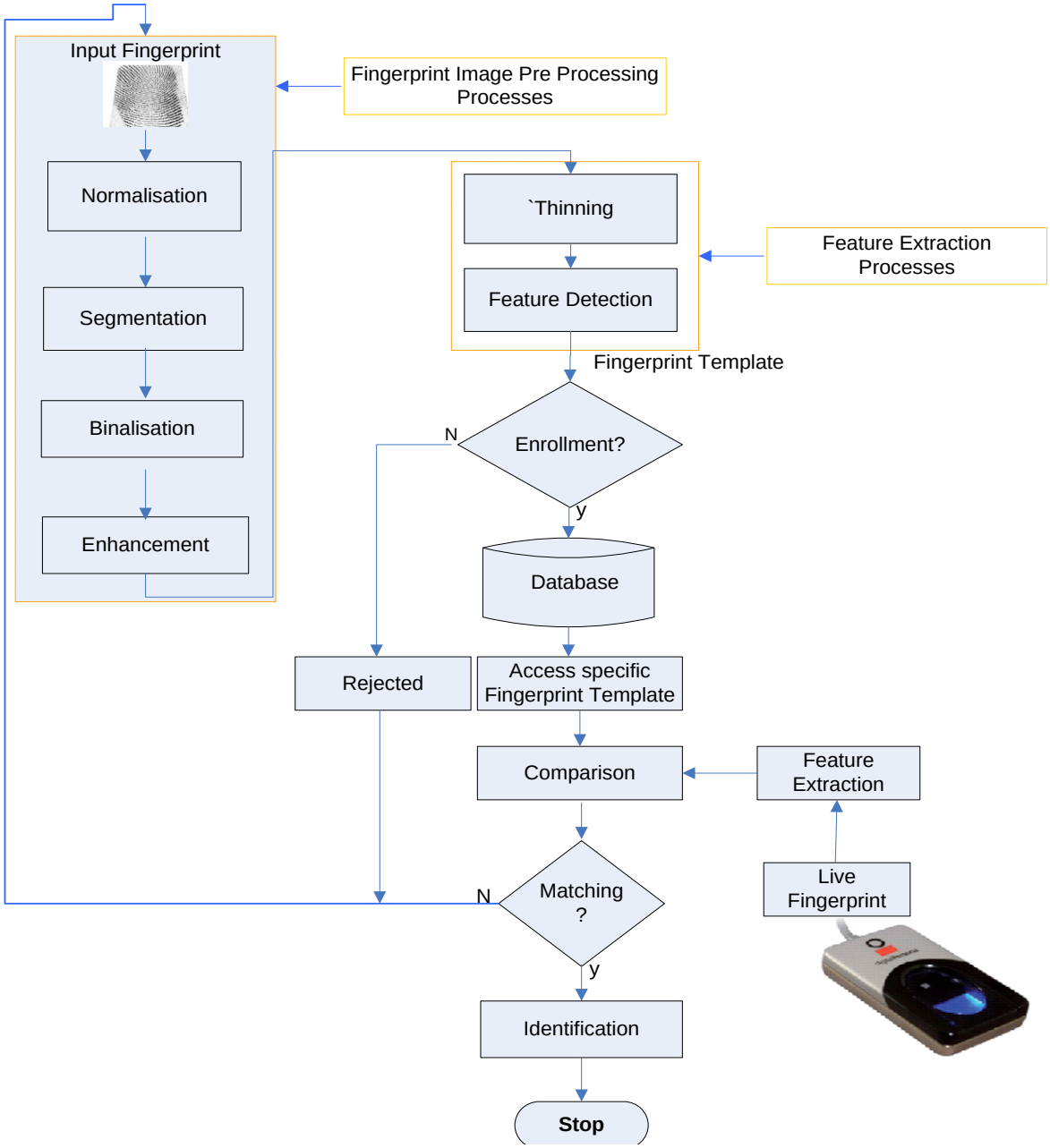


Figure 4. Data Flow Diagram of fingerprint identification system

7.3.1. Capturing

Fingerprint capturing is the process of input fingerprint image from the optical fingerprint scanner into the computer system.

7.3.2. Normalisation

Normalization operation acts on the input fingerprint image to standardize image pixel intensity values. In this study the research used image brightness normaliser filter (code). Normalisation is the pre-processing stage in fingerprint template generation and is defined by variance analysis as illustrated in equation 1:

$$N(i,j) = \begin{cases} M_0 + \sqrt{\frac{v_0\,(I(i,j)-M)^2}{v_0}} & \text{if } I(i,j) > M \\ M_0 - \sqrt{\frac{v_0(I(i,j)-M)^2}{v_0}} & \text{otherwise} \end{cases} \quad (1)$$

Where:

M and V are the estimated mean and variance of image I (i; j), respectively, and M_0 and V_0 are the desired mean and variance values, respectively.

7.3.3. Segmentation

After normalisation process of fingerprint image I, the segmentation process is performed to separate foreground

from the background image. The study implemented Otsu variance threshold method which assume that the intensity values are different in different fingerprint image and thus within each region represent the corresponding object within the scene, the intensity values are similar [12]. Threshold method was used to extract fingerprint feature from its background by assigning intensity value T (Threshold) as the function f(x,y) for each pixel P. Generally, threshold is expressed as $T = T[x, y, P(x, y), f(x, y)]$ for block Size W×W. Otsu algorithm represents grey image variance. The grey-level variance for a block of size W×W was calculated as shown in equation 2:

$$v(k) = \frac{1}{w^2} \sum_{i=0}^{w-1} \sum_{j=0}^{w-1} (I(i,j) - M(k))^2 \quad (2)$$

Where:

V (k) is the variance for block k, I (i, j) is the grey-level value at pixel (i, j), and M (k) is the mean grey-level value for the block k.

7.3.4. Enhancement

The configuration of parallel ridges and valleys with well-defined frequency and orientation in a fingerprint image provide useful information which helps in removing undesired noise. Gabor filter was appropriately applied because it has both frequency-selective and orientation-selective properties and have optimal joint resolution in both spatial and frequency domains [13]. Therefore, it was appropriate to use Gabor filters as band pass filters to remove the noise and preserve true ridge and valley structures [14].

7.3.5. Binarisation

Binalisation is the final stage in fingerprint pre-processing stages. It converts a grey level image into a binary image by improving the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of Minutiae. Let image I (x, y) represent the intensity value of enhanced grayscale image at pixel position (x, y). Let Tp be the threshold value. In case of fingerprint images Tp represents the imbalance in intensity between the back-ground pixels and ridge pixels. BW(x, y) rep-resent the binary image obtained. BW(x, y) is represented in equation 3 below:

$$BW(x,y) = \begin{cases} 1, & if\ I(x,y) \geq Tp \\ 0, & Otherwise \end{cases} \quad (3)$$

Where:

Pi is the pixel value in neighbourhood of P. The eight neighbourhood pixels are scanned anti-clockwise [11]. The results are shown in figure 5.

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Figure 5. 3x3 Window for searching minutiae [11]

The CN for ridge pixel is computed and classified according to the corresponding property value. Ridge pixel values are then classified as ridge ending, crossover, bifurcation, isolated points and crossing points as illustrated in the figure 6.

7.3.6. Enrolment Stage

During enrolment stage, biometric data are obtained, linked with identity, and encoded for storage, retrieval and matching. Fingerprint scanner is used to collect data and verify identities [1].

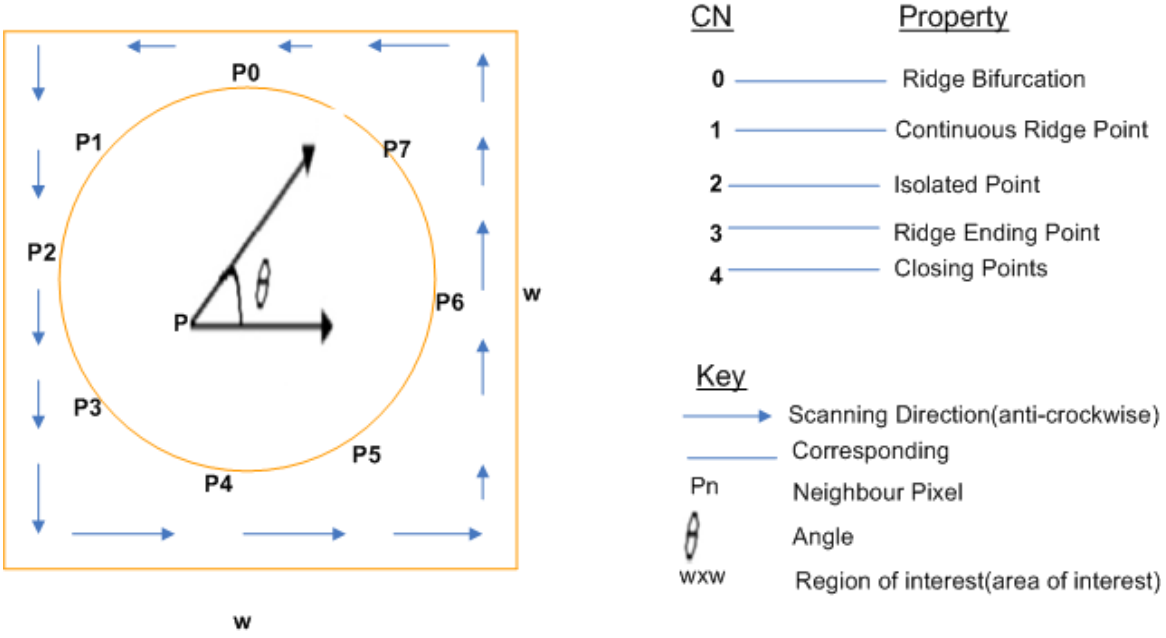


Figure 6. Crossing Number Minutiae extraction techniques

7.3.7. Identification

Identification is conducted to verify the live scanned fingerprint of an individual from that stored on the database table. The matching algorithm compares a current fingerprint image against the previous enrolled print, checking whether they come from the same finger.

7.3.8. Database Operations

Business logic also contained database operation which is sometimes refers to relational operation. Database procedure or operations is a collection of database tasks defined by end users or application code, for example, a batch job or Extraction algorithm, Transformation, and Loading (ETL) processing. The basic database operation includes insert, update, delete and search operations were implemented in the study. Other relational database operators employed include Union, Selection and append.

8. Entity Relationship Diagram (ERD)

An Entity–Relationship (ER) Model was used to define the data or information characteristics of a business domain or its process requirements. The ERD in abstract may lends to ultimate implementation in the relational database. The main components of ER models are entities (things) and their relationships. An entity is any person, place, thing, or event of interest to the organisation and about which data are captured, stored, or processed. The ERD diagram of the study consisted entities shown in figure 7:

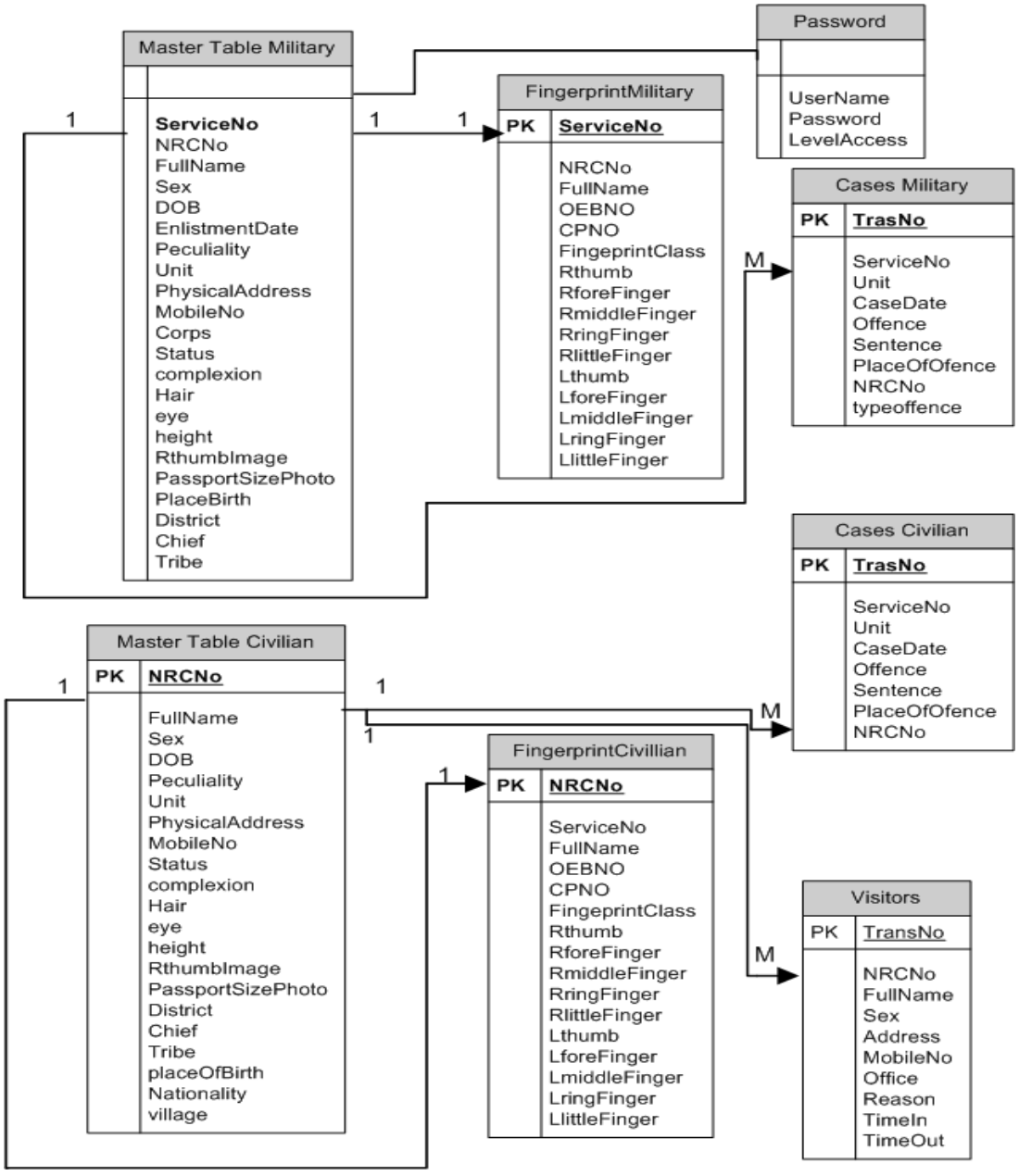


Figure 7. ERD for automatic fingerprint Identification system

9. Class Diagram

Object Oriented Analysis and design model real-world entities using class diagram [9]. In other words, class diagram Elucidates a collection of objects in the problem space through which we choose to view that space in a physical sense. The class diagram is described as a static diagram. It represents the static view of the developed application [9]. Furthermore, Class diagram was not only used for visualizing describing and documenting different aspects of a system but also for constructing executable code of the software application. Other uses include describe the attributes, operations and also the constraints imposed on the system. The class diagrams are widely employed in the software modelling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages [8]. The class diagram shows a collection of classes, interfaces, associations, collaborations and constraints. It is also known as a structural diagram [9]. Figure 8 shows class diagram of the proposed system.

10. Results

For identification purposes, verification systems require two stages of operations enrolment and identification. During the enrolment stage, biometric data are obtained, linked with known identity details, and encoded for storage, retrieval, and matching. Fingerprint scanners devices are used to collect the data. A reference template is created which is stored in the central database or decentralised portable devices like hard drives. Verification occurs when someone claims some particular identity. The biometric system compares the newly scanned information to the previously stored version. Identification is then provided or rejected. Figure 6 shows the result of enrolment process while figure 7 shows the result of identification process implementation.

10.1. Enrolment

Enrolment is a fast process and the results are credibly shown in figure 9. When the fingerprint donor presses enrol button on the screen, the dialog form enrol display automatically to prompt the name of the fingerprint donor. This is happening in step 1. In step 2, another dialog form appears automatically detailing the donor to press his/her finger on the sensor. After supplying fingerprint, enrolment process is completed and the image is saved for future use.

10.2. Verification

A guest identity may either be Verification or rejected as shown figure 10.

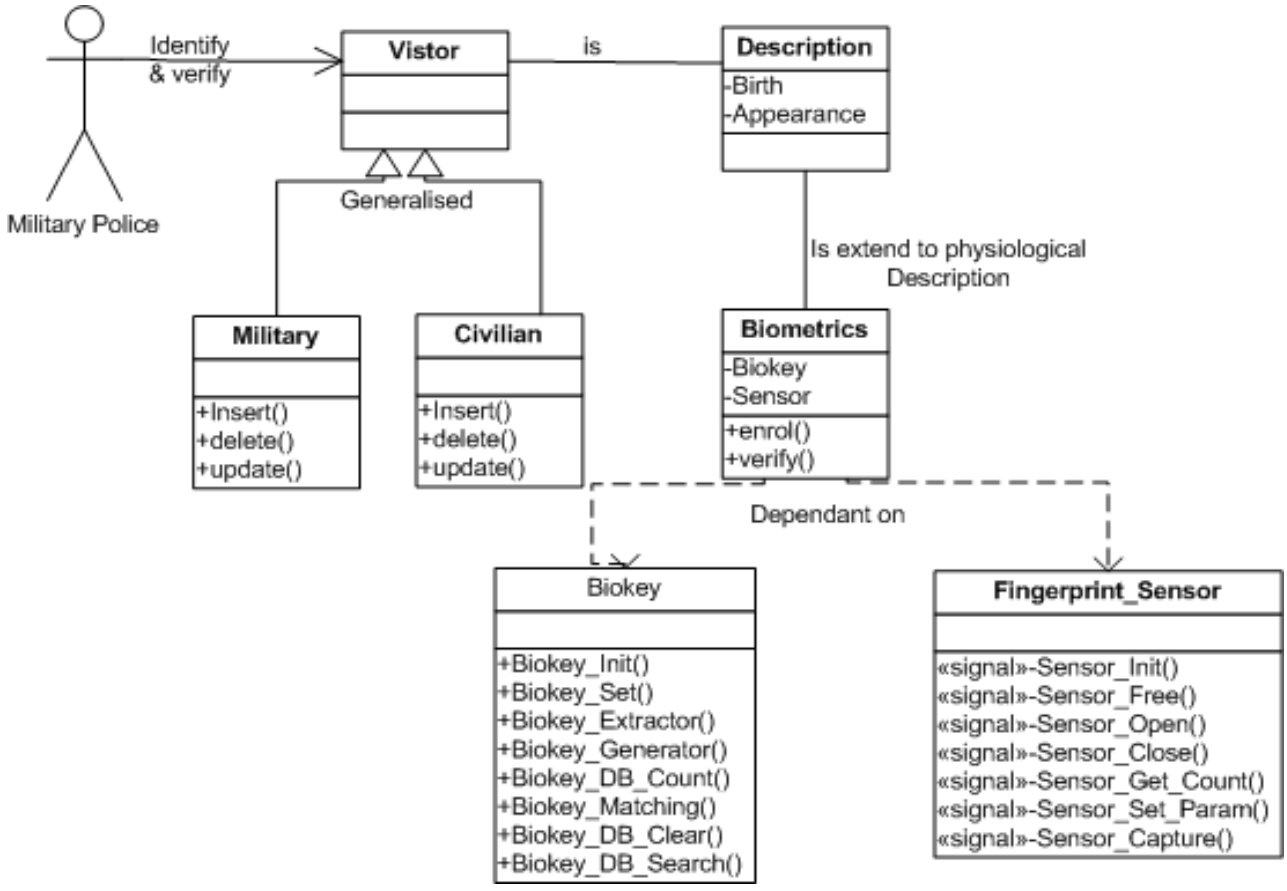


Figure 8. Class diagram for automated fingerprint biometrics system for military organization

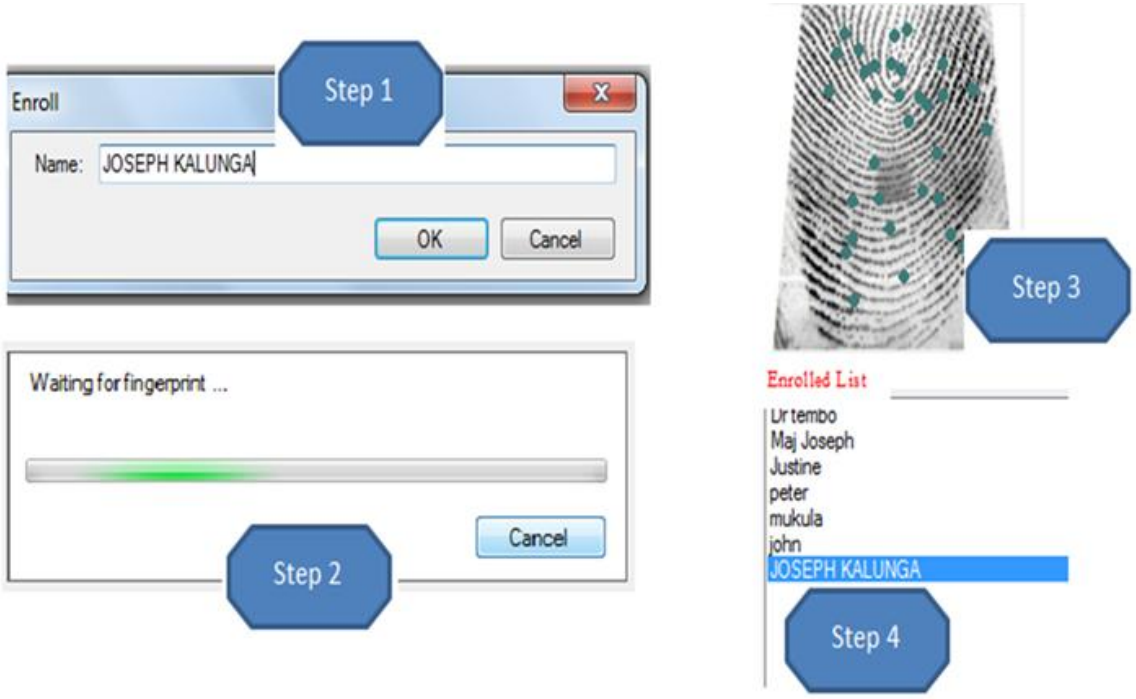


Figure 9. Fingerprint Enrollment

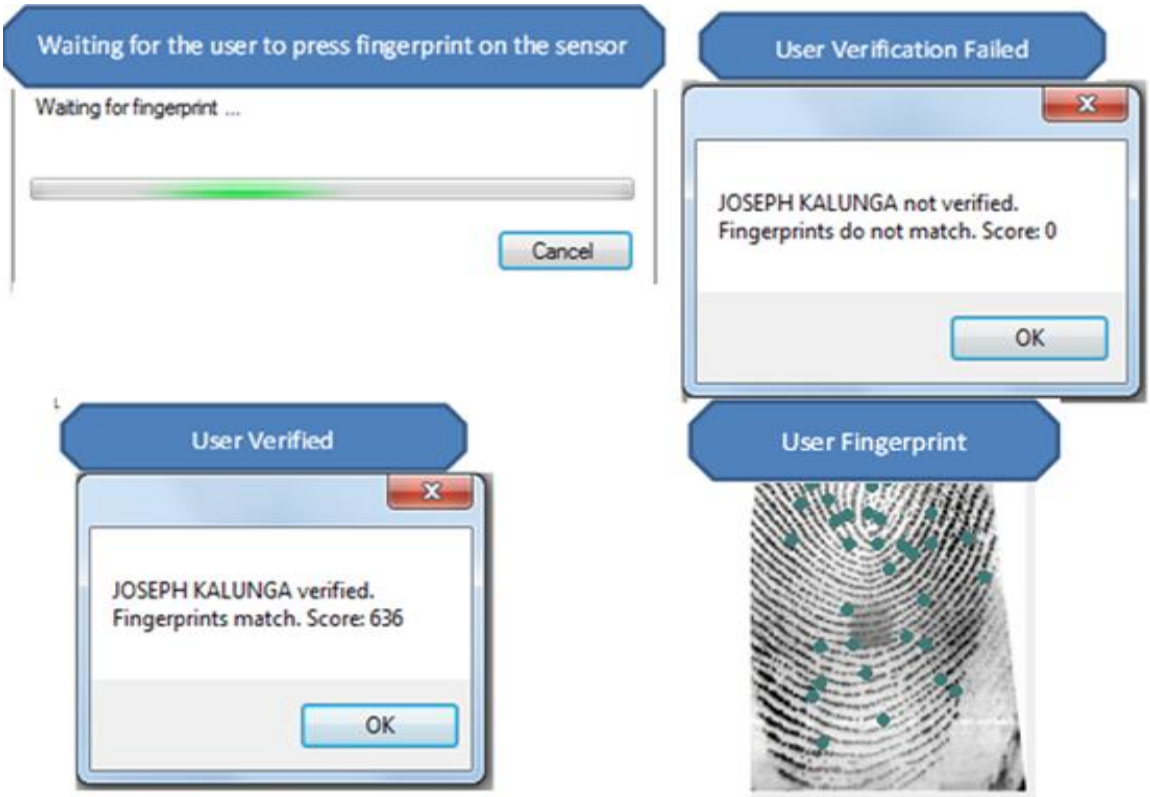


Figure 10. Fingerprint verification process

10.3. Fingerprint Analysis

Fingerprint analysis is the most commonly used requirement in criminal investigations today. It is used in sensitive institutions for forensic investigation and identification of enemies or criminal suspects who have been captured. It is also used to marry up evidence collected at crime site to original donor among those prints stored in the database. This module can also be used to detect weather stored fingerprint evidence has been tempered with. This is done by recounting the numbers of image pixels if equal to the one recorded in the database table and respected timestamp. Figure 11 illustrates fingerprint analysis screen.

Figure 11a. Fingerprint analysis screen (original)

Figure 11b. Fingerprint analysis screen (magnified)

10.4. Criminal Vetting

The criminal vetting requirement was implemented in an integrated system as presented in figure 12. Criminal vetting requires capturing of ten fingerprints together with human biographical details. Biographical (personal) are employed for human identification.

10.5. Digitalised Identity Card

The developed application automates the production of organization identification card. Organizations identity card produced is enshrined with fingerprint image and secret code which invisible to naked eyes but visible to investigator when the card is scanned or digitalized. The secret key is extracted from date of birth, national registration card number and district code where the national registration card was issued. Figure 13 shows the proposed digitalized organisation identity card.

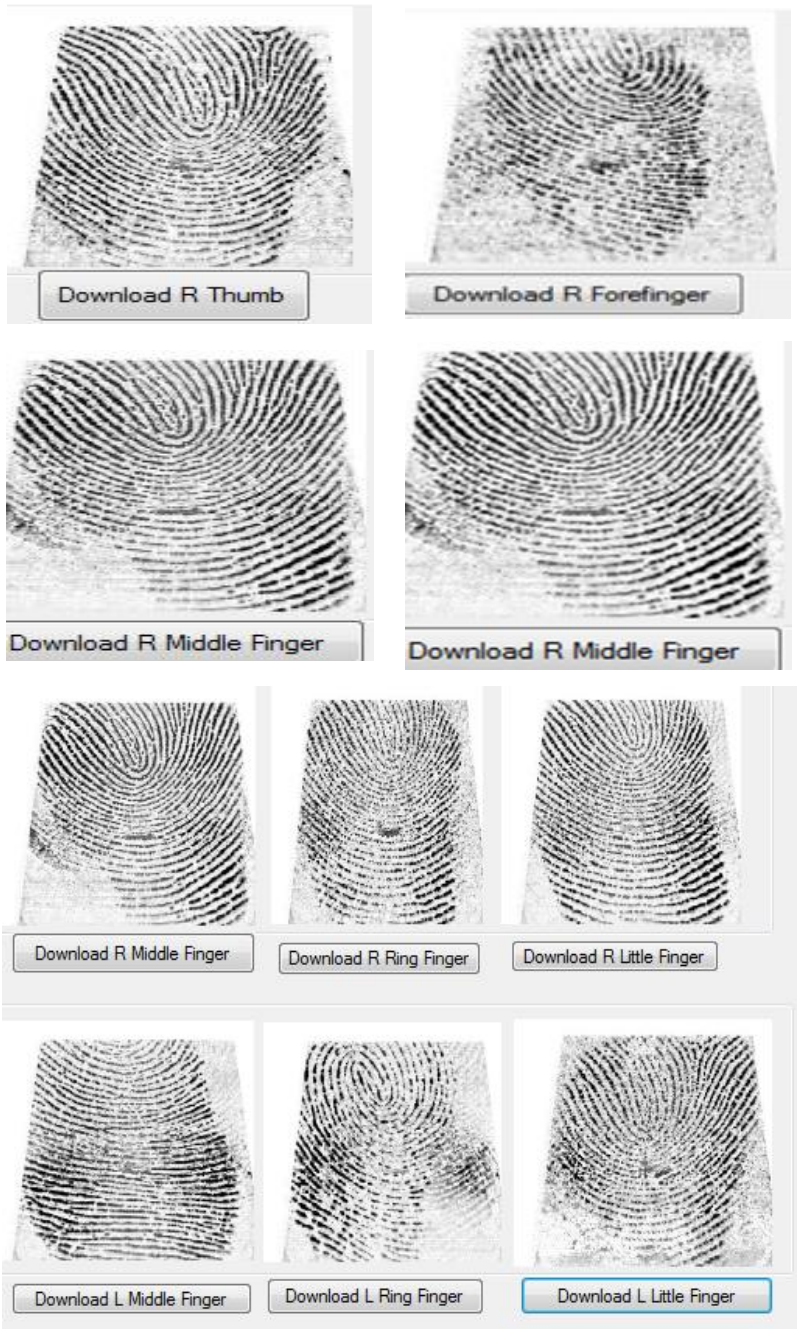


Figure 12. Criminal Vetting automated form

Figure 13. Service Identification Card

11. Performance Evaluation and Discussion

The developed system is implemented using visual studio 2010 with c# programming language, System Development Kit (SDK) version 5.0 and MySQL database. 10 fingerprint images (size 260 ×300) were scanned using digital Personal fingerprint scanner. The scanner resolution was adjusted to 300 dpi which is a prescribe FBI standard. To evaluate the performance of developed system FAR and FRR are calculated. In the first batch of 10 fingerprint enrolled, the total of 10 print were identified. In the next batch of 10 no fingerprint was rejected. In the third batch no rejection was record again. Therefore, biometric error allowance is provided for at the rate 0.001% FAR and 0.001% FRR. The accuracy level of biometric sub system is good. From preliminary results, the developed database for military has also shown good results too in terms of record management.

12. Conclusions

This paper presented the development of fingerprint authentication system for sensitive organization. Cheaper optical fingerprint scanner, open source fingerprint system development kit (SDK), visual studio 2010 and MySQL (open source) backend database was employed. Comparative study was instigated on related products especially in sensitive organization. During the study it was discovered that similar systems were developed and implemented by some security officers. Those applications improved security in respective security's operation area.

To model this application Use case diagram, activity diagram, DFDs, ERD and class diagrams were used. The Use case diagram was used to define users, roles, processes and their relationships. Activity diagram illustrated business case while data flow diagram detailed the logical flow of activities or information in the system. For example, DFDs helped us to understand the process of digital image processing in fingerprint biometric verification system. Fingerprint biometrics verification system has two important processes namely enrollment and authentication. The fingerprint image captured for minutiae based fingerprint biometrics systems under go digital image processing. Digital image processing involves image capture, normalization, segmentation, enhancement, binalisation, thinning and finally minutiae detection processes.

Coming to results, the developed application has abilities to verify an identity of human being using fingerprints. Furthermore, the system has capabilities of conduct forensics investigation based on fingerprint analysis. The developed system allow security Vetting and production of organization identity cards other capabilities are provision of data storage, retrieval and dissemination of security information.

ACKNOWLEDGEMENTS

I would like to thank Dr Simon Tembo, Head of Department, Department of Electrical & Electronic Engineering, School of Engineering at the University of Zambia,Special thanks also goes to my wife Chileshe, my daughter Mapalo and my friends. I love you guys. May God Continue Blessing you!

REFERENCES

[1] R. C. Ã, "Journal of Retailing and Consumer Services Biometric technology in retailing: Will consumers accept fingerprint authentication?," *J. Retail. Consum. Serv.*, vol. 17, no. 3, pp. 181–188, 2010.

[2] A. S. Chaudhari, G. K. Patnaik, and C. Engineering, "Implementation of Minutiae Based Fingerprint Identification System Using Crossing Number Concept," vol. 18, no. 1, pp. 17–26, 2014.

[3] J. a. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology along with trends and prospects," *Pattern Recognit.*, vol. 47, no. 8, pp. 2673–2688, 2014.

[4] T. Caldwell, "Market report: border biometrics," *Biometric Technol. Today*, vol. 2015, no. 5, pp. 5–11, 2015.

[5] L. O'Gorman, "An overview of fingerprint verification technologies," *Inf. Secur. Tech. Rep.*, vol. 4, no. 1, pp. 28–29, 1999.

[6] S. Gold, "Military biometrics on the frontline," *Biometric Technol. Today*, vol. 2010, no. 10, pp. 7–9, 2010.

[7] A. Warren and E. Mavroudi, "Surveillance and identity management: Migrant perspectives on UK Biometric Residence Permits," *Comput. Law Secur. Rev.*, vol. 27, no. 3, pp. 245–249, 2011.

[8] K. S. Adewole, S. O. Abdulsalam, R. S. Babatunde, T. M. Shittu, and M. O. Oloyede, "Development of Fingerprint Biometric Attendance System for Non-Academic Staff in a Tertiary Institution," vol. 5, no. 2, pp. 62–70, 2014.

[9] A. M. Langer, *Analysis and Design of Information Systems Third Edition British Library Cataloguing in Publication Data*. 2008.

[10] N. M. Egli, C. Champod, and P. Margot, "Evidence evaluation in fingerprint comparison and automated fingerprint identification systems — Modelling within finger variability," vol. 167, pp. 189–195, 2007.

[11] A. S. Chaudhari, G. K. Patnaik, and S. S. Patil, "Implementation of Minutiae Based Fingerprint Identification System Using Crossing Number Concept," *Inform. Econ.*, vol. 18, no. 1/2014, pp. 17–26, 2014.

[12] P. Smith, D. B. Reid, C. Environment, L. Palo, P. Alto, and P. L. Smith, "Smith et al. - 1979 - A Tlreshold Selection Method from Gray-Level Histograms," vol. 20, no. 1, pp. 62–66, 1979.

[13] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Syst. Appl.*, vol. 40, no. 5, pp. 1888–1901, Apr. 2013.

[14] J. a. Montoya Zegarra, N. J. Leite, and R. da Silva Torres, "Wavelet-based fingerprint image retrieval," *J. Comput. Appl. Math.*, vol. 227, no. 2, pp. 294–307, 2009.