UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

BIOMETRIC AUTHENTICATION

A CASE FOR THE NAIROBI SECURITIES EXCHANGE

BY

PAUL KIBIRA RURERI: P58/62312/2010

SUPERVISOR

CHRISTOPHER MOTURI

OCTOBER 2013

A Project Submitted in Partial Fulfillment of the Requirement for the Award of Masters of Science in Computer Science of the University of Nairobi

DECLARATION

This project is my original work and has not been presented for a degree in any other university.

PAUL K. RURERI (P58/62312/2010)   DATE

This Project Report has been submitted for Examination with my approval as a University Supervisor.

CHRISTOPHER A. MOTURI   DATE

DEDICATION

This work is dedicated to my wife Dorcas and our twins Samantha and Ryan. They have really inspired me. It is further dedicated to my dear parents Joseph Rureri and Josephine Rureri who used all means at their disposal to educate me.

ACKNOWLEDGEMENT

I wish to express gratitude to my supervisor Mr. Christopher A. Moturi, for taking me through this wonderful work. I highly appreciate his insights and guidance over this project work, and the encouragement he gave me throughout the whole process. Special gratitude goes to my family and staff of the various organizations where I was collecting data e.g. the stock brokerage firms who stood by me during this research.

Finally, I thank the Almighty God, and all those who have in one way or another supported me through my academic pursuit over the years.

To you all, I say thank you and may God richly reward you. Glory be to God.

ABSTRACT

There has been a sharp increase in fraud activities in various organizations in Kenya such as banks and stock brokerage firms. This has been happening mostly due to poor authentication of clients. Most of these organizations rely on identification documents like the national identification cards, written signatures, passwords and secret codes as means of authentication. Physical identification documents can be lost, stolen or misplaced. Passwords and secret codes can also be forgotten or revealed unintentionally.

This research sought a more reliable and a secure alternative means of authenticating clients by use of biometrics. The research explored and analyzed various biometric features that can be used for authentication including fingerprint, finger vein, hand geometry, retina, iris, face, DNA, among others.

The analysis of the various biometric features explored indicated that a combination of fingerprint and finger vein biometrics is more reliable, secure, and easily applicable. A multimodal biometric authentication conceptual model was developed. The model assisted in developing a multimodal authentication prototype that uses fingerprint and password. The proposed authentication prototype was to use fingerprint and finger vein biometrics but could not be developed due to lack of a finger vein scanner in the local market.

Areas that could be prone to attacks in the developed prototype were identified and various measures like data encryption were put in place to avoid the attacks.

Contents

LIST OF TABLES

LIST OF FIGURES

DEFINITION OF IMPORTANT TERMS

Biometrics

It is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, veins, eye retinas and irises, voice patterns, facial patterns and hand measurements, for authentication purposes

Authentication

It is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Multimodal Biometrics

They are technologies that are capable of using more than one physiological or behavioral characteristic for enrollment, verification or identification.

CHAPTER 1: INTRODUCTION

1.1 Background

There have been several cases of people who impersonate others and instruct stock brokerage firms to sell shares of an innocent client. The fraudsters achieve this by presenting falsified identification documents like the national identification cards or passports. They even go ahead and falsify the signatures of the targeted clients. Currently most of the stock brokerage firms rely on hand written signature of the shareholders and their national identification cards or passports as the only means of authentication.

1.2 Problem Statement and Purpose of the Project

Criminals are using modern technologies to falsify identification documents in a way that it is hard to differentiate between the original one and the fake one. Physical identification documents like the national identifications cards and passports can be misplaced or stolen. On the other hand the use of passwords and security codes as a means of authentication is only secure up to some extent because there may be a chance of revealing the password either by force or without knowing or sometimes the authorized person may forget the password. Use of handwritten signatures has also become prone to forgery especially for people who write simple signatures. Handwritten signatures are also not very reliable because human beings can forget how their signatures looks like if they stay for long without signing. Forgetting ones signature can deny you the opportunity of transacting your business if the signature signed does not match with the one in the database

1.3 Research Objectives

The following were the specific objectives of this study:

1. Explore and analyze various biometric characteristics used for authentication.
2. Develop a reliable and secure multimodal authentication prototype.
3. Identify areas in the authentication prototype that can be prone to attacks and how they can be avoided and managed.

1.4 Research Questions

This research intended to address the following questions:-

1. What were the various biometric characteristics used for authentication?
2. What were the pro and cons of the various biometric characteristics?

3. Which combination of the various characteristics could make the most secure and reliable multimodal authentication?
4. What were the challenges that could have affected the successful implementation of a biometric authentication system?

1.5 Justification and Significance of the Study

Due to the increased forgery and impersonation in stock exchange firms nowadays, a more secure authentication system is therefore required. The system should not be vulnerable to forgery and impersonation as it is the case in written signatures, identification tokens and passwords. Every person has unique physical biometrics, such as fingerprints, veins, hand geometry, retina, iris, and facial characteristics which cannot be removed, changed or forgotten and therefore they can be an ideal means of identification. Biometric authentication technology therefore can provide a more secure and reliable way of verifying real users. This technology is easy to implement because what Securities Exchange firm needs to do is to register shareholders' biometric characteristics in their system and store the images in a database. Every time a client comes to do a transaction to his or her account the authentication system scans his or her biometric features and then looks for a match from the database. If a match is found the client is allowed to transact else he or she is denied.

1.6 Scope, Limitations and Assumptions

The research was conducted in 17 members of the Nairobi Securities Exchange located in Nairobi city. To gain an expert view of biometric authentication, the study involved a few biometric experts located in Nairobi.

The major limitations were:

1. Some biometric devices were too expensive while others were not locally available.
2. Some of the respondents were not willing to give all the required information considering the sensitivity of the matter.
3. Only 3 biometric experts were involved in the study due to their limited availability.

Assumptions:

The researcher had the following assumptions when carrying out the study:

1. That it was possible to get at least 3 biometric experts in Nairobi.
2. That the 17 member firms of the Nairobi Securities Exchange were willing to give out information as required.

3. That the 17 member firms of the Nairobi Securities Exchange had key personnel's with ability to respond to research questions.
4. That the required biometric devices were available in the market

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

Biometrics are technologies used for measuring and analyzing a person's unique characteristics, (www.biometricnewsportal.com). There are two types of biometrics: behavioral and physical. Behavioral biometrics are generally used for verification while physical biometrics can be used for either **identification** or **verification**.

Identification is determining who a person is. It involves trying to find a match for a person's biometric data in a database containing records of people and that characteristic. This method requires time and a large amount of processing power, especially if the database is very large.

Verification is determining if a person is who they say they are. It involves comparing a user's biometric data to the previously recorded data for that person to ensure that this is the same person. This method requires less processing power and time, and is used for access control (to buildings or data).

Commonly the main physical biometric technologies that have been used include the fingerprint, iris, retina, hand, palm vein and face. A biometric system usually consists of a scanner / reader that capture the user's biometrics characteristics, a piece of software that converts this data into digital form and compares it with data previously recorded and a database, which stores the biometric data

Bhattacharyya *et al.* (2009) did a review on "*Biometric Auth*entication". In their review Bhattacharyya *et al.* (2009) noted that information security needs to be given a serious attention considering the advances in the field of Information Technology. They have pointed out that one way of securing information systems is by the use biometric authentication techniques to determine the identity of an individual requesting some services.

Their review shows the reliability of biometric authentication by giving reasons that physical human characteristics are not easy to falsify as compared to security codes, passwords, and tokens such as identification cards which can be lost, stolen, duplicated or forgotten at home. Passwords and security codes can be forgotten, shared or observed.

Although they conclude by indicating that biometric authentications can only offer a high degree of security if sound principles of system engineering are put in place, they fail to show in details how these principles can be applied.

2.2 Implementation Process of Biometric System

The implementation process of a biometric system involves the following two stages, *(www.bromba.com)*:

1. Biometric enrollment
2. Biometric recognition

Biometric Enrollment

To be able to recognize a person by their biometric characteristics and the derived biometric features, first a learning phase must take place. The procedure is called enrolment and comprehends the creation of an enrolment data record of the biometric data subject (the person to be enrolled) and to store it in a biometric enrolment database (Fig. 1). The enrolment data record comprises one or multiple biometric references and arbitrary non-biometric data such as a name or a personnel number.

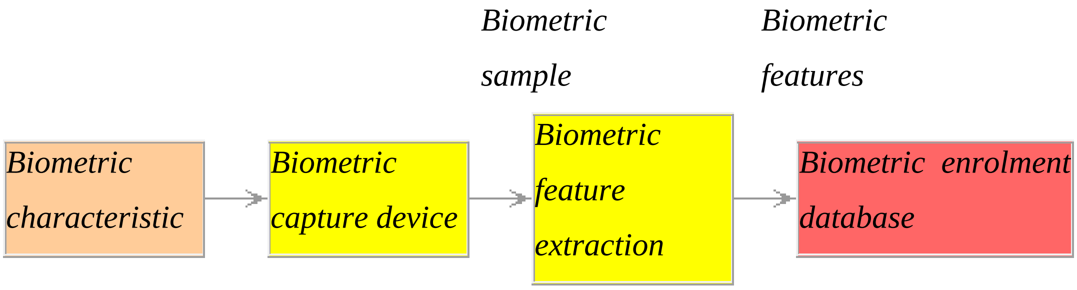


Fig. 1. Typical Internal Enrolment Process (www.bromba.com)

Biometric Recognition

For the purpose of recognition, the biometric data subject (the person to be recognized) presents his or her biometric characteristic to the biometric capture device which generates a recognition biometric sample from it. From the recognition biometric sample the biometric feature extraction creates biometric features which are compared with one or multiple biometric templates from the biometric enrolment database (Fig. 2). Due to the statistical nature of biometric samples there is generally no exact match possible. For that reason, the decision process will only assign the biometric data subject to a biometric template and confirm recognition if the comparison score exceeds an adjustable threshold.

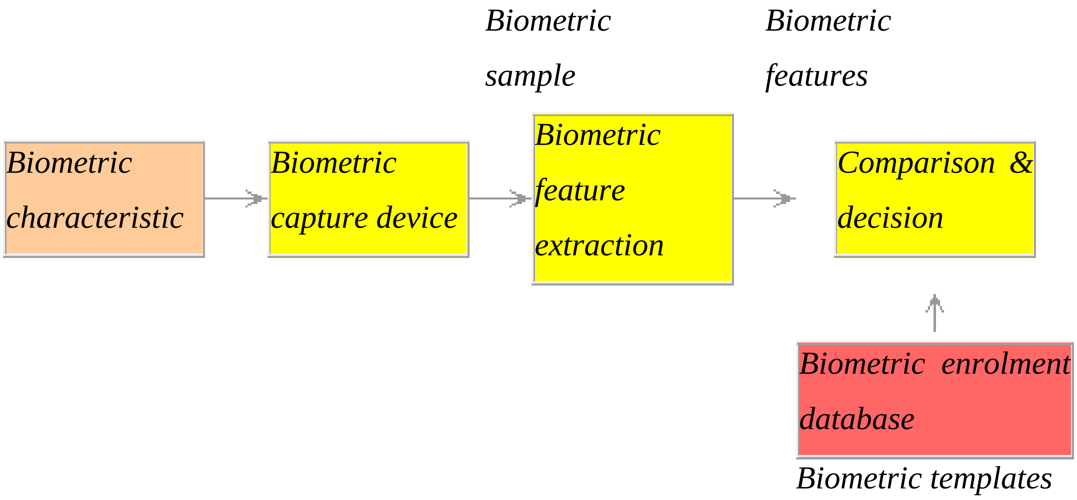


Fig. 2. Typical Biometric Recognition Process (www.bromba.com)

2.3 Challenges of a Biometric System

Although biometric technology has proved to be reliable in verification and identification of persons, some studies has revealed three issues associated with this technology as follows:

1. The false accept rate (FAR)
2. The false reject rate (FRR)
3. Compromised biometric data

A False Accept is when a nonmatching pair of biometric data is wrongly accepted as a match by the system. A False Reject is when a matching pair of biometric data is wrongly rejected by the system. The two errors are complementary: When you try to lower one of the errors by varying the threshold, the other error rate automatically increases. There is therefore a balance to be found, with a decision threshold that can be specified to either reduce the risk of FAR, or to reduce the risk of FRR.

In a biometric authentication system, the relative false accept and false reject rates can be set by choosing a particular operating point (i.e., a detection threshold). Very low (close to zero) error rates for both errors (FAR and FRR) at the same time are not possible. By setting a high threshold, the FAR error can be close to zero, and similarly by setting a significantly low threshold, the FRR rate can be close to zero. A meaningful operating point for the threshold is decided based on the application requirements, and the FAR versus FRR error rates at that operating point may be quite different. To provide high security, biometric systems operate at a low FAR instead of the commonly recommended equal error rate (EER) operating point where FAR = FRR.

The greatest strength of biometrics is at the same time its greatest liability. It is the fact that an individual's biometric data does not change over time: the pattern in your iris, retina or palm vein remain the same throughout your life. Unfortunately, this means that should a set of biometric data be compromised, it is compromised forever. The user only has a limited number of biometric features (one face, two hands, ten fingers, two eyes). For authentication systems based on physical tokens such as keys and badges, a compromised token can be easily canceled and the user can be assigned a new token. Similarly, user IDs and passwords can be changed as often as required. But if the biometric data are compromised, the user may quickly run out of biometric features to be used for authentication.

2.4 Vulnerabilities and Performance Analysis

Guillen *et al.* (2012) conducted a study on "*Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network"*. In order to understand the vulnerabilities in fingerprint biometric systems, they analyzed the evaluation process for fingerprint recognition system in two parts. The first part is analysis about the biometric fingerprint system itself, while the second part is analysis about the database server, the developed application, the fingerprint scanner and the network in general.

The study further says that attacks to the biometric identification systems are classified into two big groups. One being direct attacks, while the other being indirect attacks. Direct attacks occur when physical devices are directly attacked. The study says false fingerprint and damage to the sensor are direct attacks. Indirect attacks occur when authentication systems are infringed by illegal accessing the communication channels to extract or modify the information in the database. The study further says indirect attacks are achieved through sniffing, hill climbing, trojans, inverse engineering and snooping. The study therefore recommends that fingerprint biometric systems need to be tested for such vulnerabilities before they can be deployed. Results of such test evaluations will help detect any risk in the system and hence allow the developer and users of the system to make a decision about the biometric system to be implemented.

2.5 Improving the Accuracy of Biometrics

Arunkumar, and Malathy, (2010), indicated in their research that, unimodal systems are not fully capable of resisting spoof attacks because of their many disadvantages. They have shown a multimodal system of fingerprint and finger vein images fused to obtain a complicated image which is very hard to duplicate and proves itself to be hundred percent resistant to spoof attack.

Sasidhar *et al.* (2010) did a study on "*Multimodal Biometric Systems"* that aimed at improving accuracy and performance. The study recommends the use of multimodal biometric systems over unimodal ones. The study shows that unimodal biometric solutions have limitations in terms of accuracy, enrolment rates, and susceptibility to spoofing. According to the study, multimodal biometric systems utilize more than one physiological or behavioural characteristic, such as fingerprints, eye retinas, and irises, voice patterns, facial patterns and hand measurement for authentication purposes.

The study has a limitation of showing which physiological or behavioural characteristic can be used together to make the best combination. The study only demonstrates the use of face and fingerprint multimodal system but does not indicate its advantages over the others.

Aboalsamh, (2009), noted that fingerprint biometric authentication alone may not achieve the high level of security required. The author therefore recommends additional use of finger vein biometrics technology to supplement the fingerprint authentication. The author compares popular biometrics as shown in Tables I and II below.

Table I. Biometrics Parameters Explained

1.	**Universality**	Each person should have the characteristic.
2.	**Uniqueness**	Is how well the biometric separates individuals from another.
3.	**Permanence**	Measures how well a biometric resists aging and other variance over time.
4.	**Collectability**	Ease of acquisition for measurement
5.	**Performance**	Accuracy, speed, and robustness of technology used.
6.	**Acceptability**	Degree of approval of a technology.
7.	**Circumvention**	Ease of use of a substitute.

Source: Aboalsamh, (2009), "*Vein and Fingerprint Biometrics Authentication- Future Trends"*

Table II. Comparison of Biometric Technologies

	Biometrics Parameters as shown above						
Biometrics	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Face	High	Low	Med	High	Low	High	Low
Fingerprint	Med	High	High	Med	High	Med	High
Hand Geometry	Med	Med	Med	High	Med	Med	Med
Iris	High	High	High	Med	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Med	Low	Low	Med	Low	High	Low
F. Thermogram	High	High	Low	High	Med	High	High
Retinal Scan	High	High	Med	Low	High	Low	High
Vein	High	Med	Med	Med	High	Med	Low

Source: Aboalsamh, (2009), "*Vein and Fingerprint Biometrics Authentication- Future Trends"*

From the comparison, it's clear to see why fingerprint and vein authentication biometrics are attractive alternatives in comparison to other biometrics.

Aboalsamh, (2009), further explains how vein biometrics technology is done. He says a set of light emitting diodes (LEDs) generates near infrared light that penetrates the body tissues. An image of the veins pattern is revealed as the near infrared light is reflected in the haemoglobin in the blood. A Charge Coupled Device (CCD) camera uses a small, rectangular piece of silicon to receive incoming light. It is now that the CCD captures the image of the vein pattern through this reflected light. The image is then processed through an algorithm to construct a finger vein pattern from the camera image and the pattern then digitized and saved as a template for biometric authentication.

Aboalsamh, (2009), study recommends the use of finger vein biometric authentication for many reasons such as no property of latency since vein patterns in fingers stay where they belong and where no one can see them, vascular sensors are both durable and usable since sensors are looking below the skin and they simply don't have issues with finger cuts, moisture or dirt. The finger vein systems are near contactless and easy to use as they are fairly intuitive and require very little training on the part of the user.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

This section presents an overview of the methods and procedures used in the study. It covers research design, population, sample and sampling techniques, data collection and analysis.

3.2 Research Design

A research design is the conceptual structure within which research is conducted. It is the overall strategy that one chooses to integrate the different components of a study in a coherent and logical way, thereby, ensuring one effectively address the research problem; it constitutes the blueprint for the collection, measurement, and analysis of data. This study has adopted a survey research design that seeks to investigate the study variables without manipulating any of them or tampering with them in an attempt to understand, describe and explain the use of biometric authentication system in the Nairobi Securities Exchange. The design was based on both descriptive qualitative and quantitative design approach depending on the type of survey questions asked i.e. closed or open ended questions.

3.3 Population

To assess the effectiveness of using biometric technology in the Nairobi Securities Exchange, the researcher got views from the stock exchange firms, which are the custodian of customer's shares and also the owner's of authentication systems, the customers, who are the owner's of the shares, and finally biometric experts who gave expert advice on use of biometrics.

The targeted population for the study thus included:

1. Members Firms of the Nairobi Securities Exchange
2. Shareholders
3. Biometric Experts

3.4 Sampling and Sampling Technique

The researcher adopted the survey type of research in which a sample from the target population was used for the study. The Nairobi Securities Exchange (NSE) website, *(www.nse.co.ke),* indicated that there are 19 licensed member firms of the NSE. The research covered 17 out of the 19 firms since 2 of the firms were under statutory management. It is from this population that the study selected key people as respondents.

The details of the sample are as follows

- 1 Person handling information technology and information systems security duties in each of the 17 firms.
- 1 System Developer in each of the 17 firms.
- 1 Person handling customer care in each of the 17 firms
- 1 system administrator in each of the 17 firms
- 1 Database administrator in each of the 17 firms
- 3 Customers in each of the 17 firms
- 3 Biometric Experts working in Nairobi

Thus in total, a sample of 139 elements were selected from the targeted population.

3.5 Data Collection

The focus of the study was on assessment of how biometric technology can be used effectively in security exchange firms, and therefore primary data from the parties involved in this matter is crucial. However, secondary data from relevant publications and internet was also collected to augment the studies.

3.6 Data Collection Methods

The researcher collected data by administering questionnaires and conducting interviews. Most of the questions were structured and aimed at covering the objectives outlined in this document. Some of the structured questions were the close-ended type and respondents were asked to mark the appropriate box matching his or her opinion. Other questions however, required respondents to give their open opinions. The research also carried out observations to see what was happening on the ground.

3.7 Data Analysis

Quantitative data collected using closed-ended questions were analyzed using statistical methods. Microsoft Excel was used to analyze the data and obtain percentages, means and frequencies. The findings were presented in form of tables, pie charts and bar graphs. Qualitative data collected using non structured questions and observations were first organized into groups and categories. Patterns within the data were identified and analyzed. Inferences and suggestions were made based on the findings.

3.8 Limitations of the Methodology

The methodology to be used in this research used both questionnaires and interviews as data collection tools. Questionnaire as a data collection tool had the following limitations:

a) Answers tend to be limited in information which can result in low validity
b) Limited depth in answers
c) Some questionnaires were not returned at all
d) Some questions were not fully understood by those answering them
e) Complex questions were difficult to use as answers would be complicated

Interviews on the other hand had the following limitations:

a) They were time consuming
b) Questions needed to be pre-planned so that all participants are asked the same questions
c) Having the interviewer present may have influenced the answers given
d) Detailed and quantitative data were difficult to analyze and interpret

CHAPTER 4: RESEARCH FINDINGS AND DISCUSSION

4.1 Response Rate

One hundred and thirty nine questionnaires were sent out and one hundred and thirteen were returned.

4.2 Background Information of the Respondents

The respondents were asked questions regarding their position/role in the organization, level of education and training and gender. This was for the purpose of gaining understanding of their capability to respond with reasonable validity and reliability to the survey.

4.3 Characteristics of the Respondents

4.3.1 Career or Role Played by the Respondent in Terms of Stock Exchange

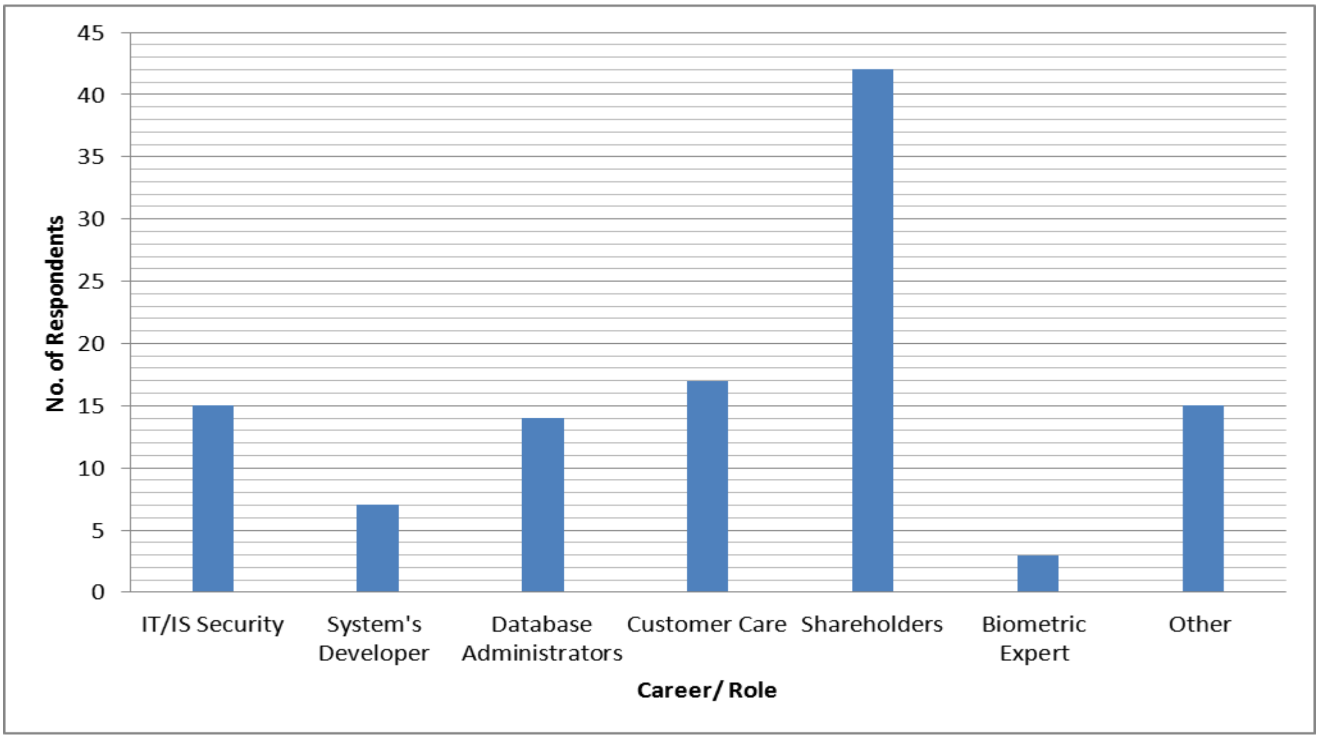


Fig. 3: Respondent’s Career/Role

The above composition brought a broad understanding of views and opinions expressed by people playing different roles in the stock market in terms of client’s authentication.

4.3.2 Highest Level of Education of the Respondents

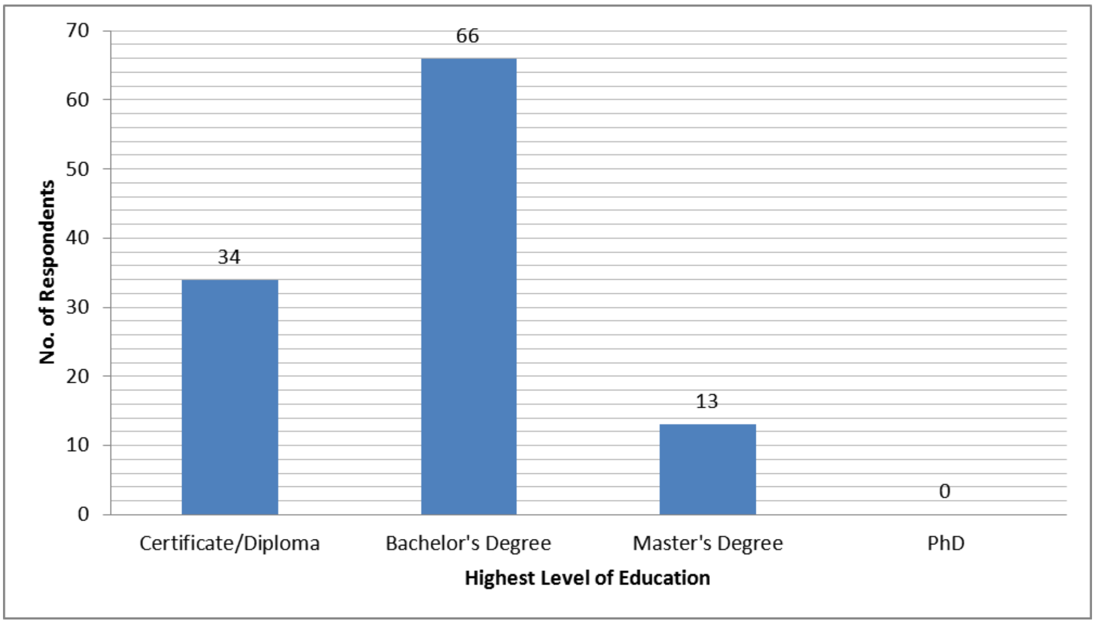


Fig. 4: Respondent’s Level of Education

Most of the respondent had attained good level of education with majority having a Bachelor’s Degree (Fig. 4). This gives some assurance that the respondents were able to understand and respond to the questions asked in the questionnaire.

4.4 Respondents Awareness of Impersonation and Fraudulent Activities in the Stock Business

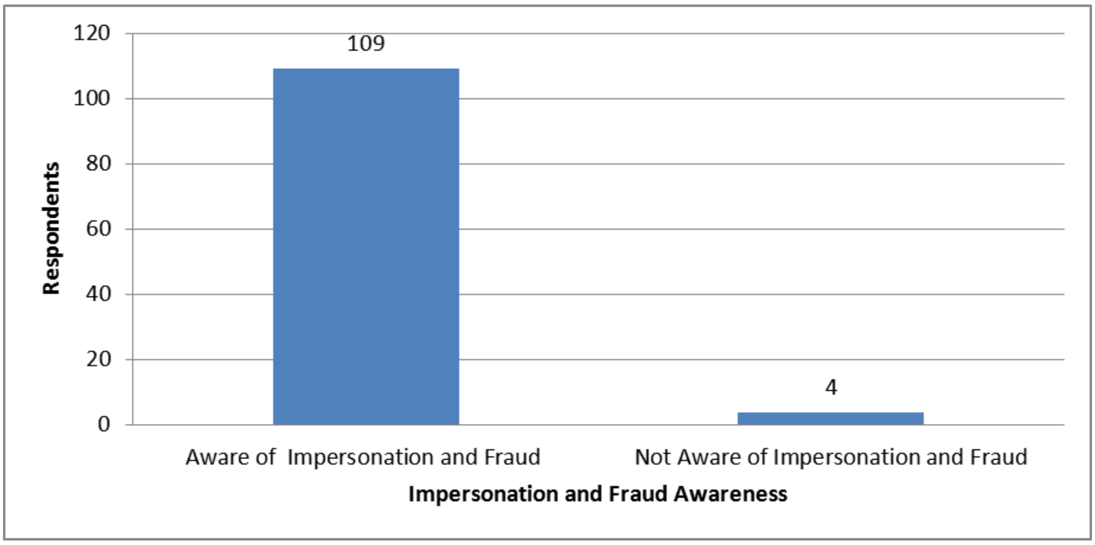


Fig. 5: Awareness of Impersonation and Fraud

Majority of the respondents indicated that they have either experienced or heard of someone lose shares to fraudulent people pretending to be the real owners of stock (Fig. 5). This particular finding shows that fraudulent activities are on the rise and so many people have fallen victims. The research further established that most investment banks experience a lot of these fraudulent cases but they decide to deal with the matter quietly without going to a court of law in order to avoid losing investors' confidence. Most of the fraudulent cases happen as a result of impersonation where criminals present stolen or fake authentication tokens.

4.5 Verification and Authentication of Clients in the Brokerage Firms

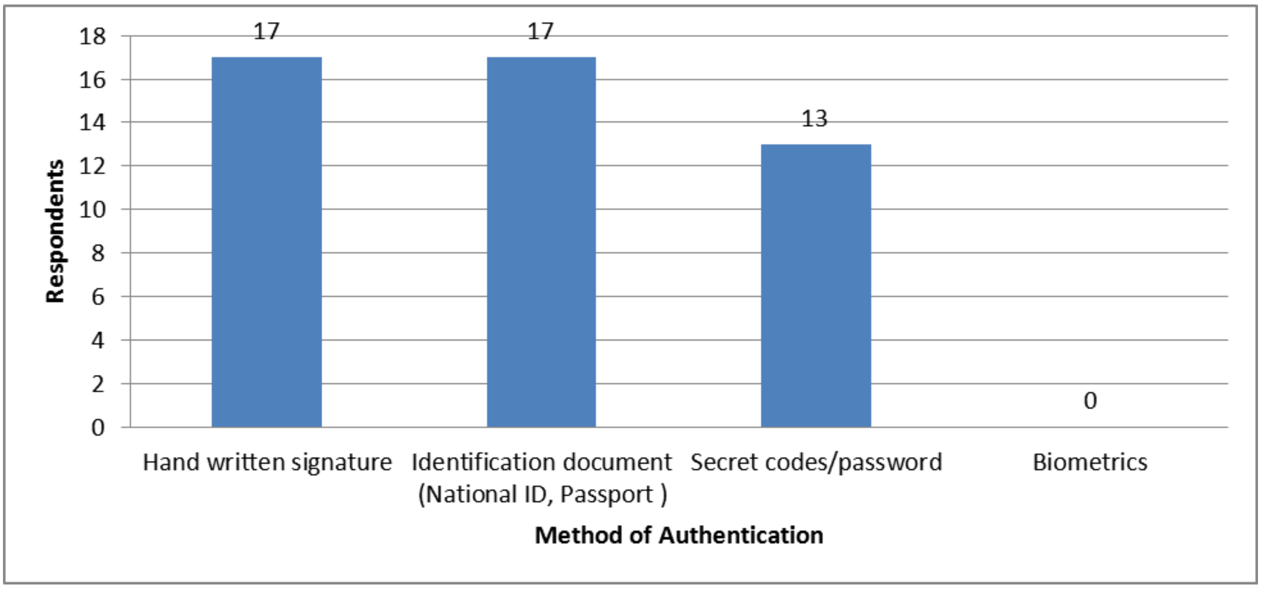


Fig. 6: Authentication Methods used in Brokerage Firms

All stock brokerage firms' use hand written signature and identification documents like the national identification card or passport to authenticate clients. 13 of them further use secret codes or passwords to authenticate clients if the client is transacting remotely via a web based system. None of the firms use biometrics as a way of authenticating clients (Fig. 6).

4.6 Reliability of the Authentication Methods used by the Brokerage Firms

Most of the respondents indicated that the current methods being used by brokerage firms are not highly reliable and secure because things like hand written signatures and identification cards are being falsified to an extent that it is hard to differentiate between the original and the fake one. Secret codes and password on the other hand are not secure because they can be revealed through eavesdropping. Identification documents like the National ID cards and passport can also be lost or forgotten at home and hence not always reliable. The respondents also indicated that most of their clients who use secret codes and password keep on forget them especially if they stay for a long time before using them.

4.7 Most Reliable and Secure Combination of Biometric Features that can be used for Client's Authentication

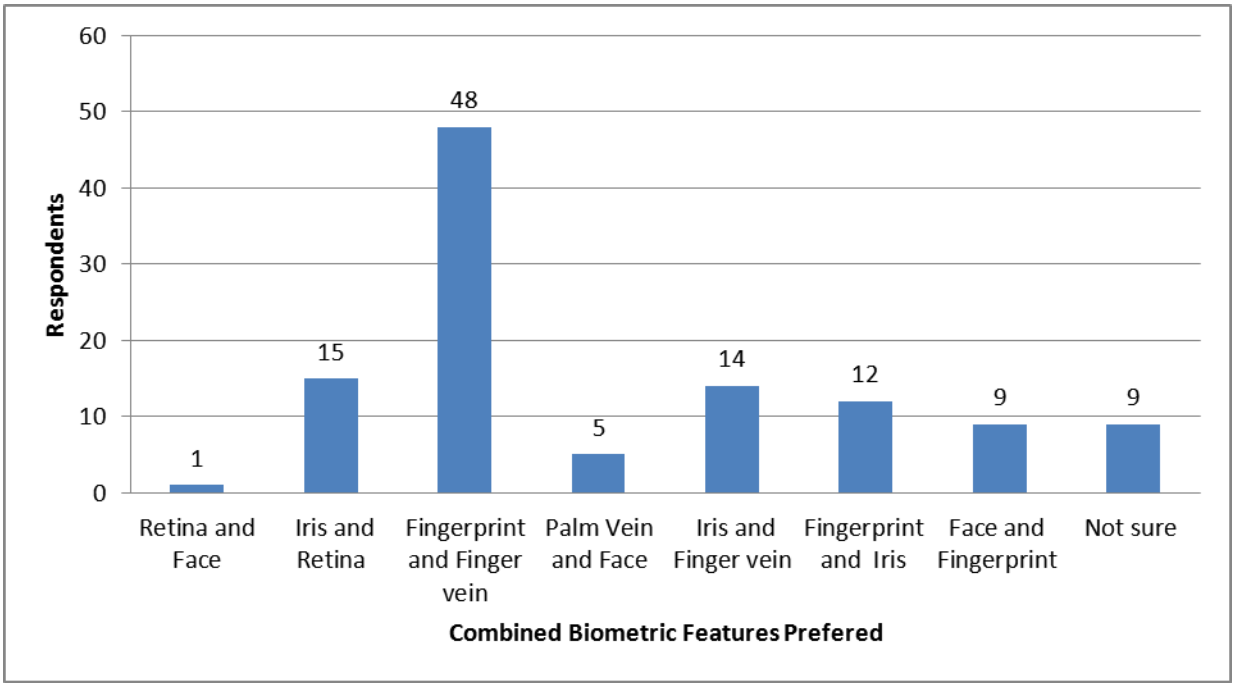


Fig. 7: Preference of Most Reliable and Secure Combined Biometric Features

It emerged that most respondents find the fingerprint and finger vein to be more reliable and secure because they are unique throughout one's life, harder to falsify and not intrusive (Fig. 7). Most of the respondents said that features like the iris and retina can be secure to use but are not reliable because many people may not accept to use them because their scanning process is very intrusive. Other respondents indicated that face recognition has a very low level of reliability because it changes over time and can be obstructed by things like glasses, hair and scarves.

4.8 Biometric Features Explored and their Pros and Cons

The following biometric features were explored when carrying out the research and their pros and cons were identified as shown below.

a) **Facial Recognition:**

Facial recognition is an automated method to record the spatial geometry of distinguishing features of the face. Different methods of facial recognition focus on measures of key features. No cooperative behavior by the user and environmental factors, such as lighting conditions, can degrade performance for facial recognition technologies. Facial recognition is non-intrusive and no contact is required. The limitations of facial recognition include obstruction by hair, glasses, hats, scarves etc, it is also sensitive to changes in lighting, expression and poses. The face of human beings also changes with time hence not very reliable to use.

b) **Voice Recognition:**

Voice recognition is an automated method of using vocal characteristics to identify individuals using a pass-phrase. The technology itself is not well-developed, partly because background noise affects its performance. Voice recognition can be affected by an illness such as a cold which can change a person’s voice, making absolute identification difficult or impossible. A person’s voice can be easily recorded and used for unauthorized purpose. Additionally, it is unclear whether the technologies actually recognize the voice or just the pronunciation of the pass-phrase (password) used to identify the user. A telephone or microphone can serve as a sensor, which makes this a relatively cheap and easily deployable technology. Voice recognition is contactless and non-intrusive and therefore has high level of social acceptability.

c) **DNA:**

Except for identical twins, each person’s DNA is unique. It can thus be considered a ‘perfect’ modality for identity verification. DNA identification techniques look at specific areas within the long human DNA sequence, which are known to vary widely between people. The accuracy of this technique is thus very high, and allows both identification and verification. Enrolment can be done from any cell that contains a nucleus; for instance taken from blood, semen, saliva or hair samples which is considered intrusive by many users. However, DNA as a biometric for identification uses a very small amount of non-coding genetic information which does not allow deciphering a person’s initial genetic heritage. At present, DNA analysis is performed in specialized laboratories and is expensive and time-consuming (roughly 4 or 5 hours for the whole procedure). Moreover, the complete lack of standardization means interoperable systems are a long way off. Moreover, DNA techniques are currently being used by Law enforcement. Thus, any wider deployment of DNA-based biometric techniques in the future, if these do indeed become quicker and cheaper, will always face acceptability problems.

d) **Retinal Scanning:**

Retinal scans measure the blood vessel patterns in the back of the eye. The device involves a light source shined into the eye of a user who must stand very still within inches of the device. Because the retina can change with certain medical conditions, such as pregnancy and high blood, this biometric has the potential to reveal more about individuals than only their identity. There is no known way to replicate a retina and therefore it accuracy level is very high. Because users perceive the technology to be intrusive, retinal scanning has lost popularity with end-users. It is also very expensive

e) **Iris Recognition:**

Iris recognition has a high level of accuracy because the iris is a protected internal organ whose random texture is stable throughout life. It can serve as a kind of living passport or a living password that one need not remember but can always present. Being that the iris is an internal organ of the eye, the iris is immune (unlike fingerprints) to environmental influences, except for its papillary response to light.

Iris scanning measures the iris pattern in the colored part of the eye (although the color has nothing to do with the scan). Iris patterns are formed randomly. This means no two iris patterns are the same; the iris pattern of one’s left eye is different from the iris pattern of the right eye. Iris scans can be used for both identification and verification applications. However, this method is relatively expensive and unavoidably involves the scanning of the eye, which makes it intrusive. Its reliability, however, means it can be successfully used both for identification and authentication (verification), an advantage which few other techniques can offer.

f) **Hand/Finger Geometry:**

Hand or finger geometry is an automated measurement of many dimensions of the hand and fingers. Neither of these methods take prints of the palm or fingers. Rather, only the spatial geometry is examined as the user lays his or her hand on the sensor’s surface and uses guiding poles between the fingers to place the hand properly and initiate the reading. Finger geometry typically uses two or three fingers. Hand geometry is a well-developed technology that has been thoroughly field-tested and is easily accepted by users.

Hand geometry recognition relies on measuring the structure of the hand. The acquisition stage takes measurements of almost 100 points on the top of the hand (size of knuckles, length of fingers, etc.) and computes a mathematical formula based on those measurements to create the template. The cooperation of the individual is required at this stage. Users tend to find hand recognition systems simpler to use because the readers are more intuitive. In addition, such systems do not hold negative connotations; thus facilitating user acceptance.

The hand's lower level of distinctiveness compared to other biometrics makes it suitable for verification and medium-scale identification applications. Compared to other biometrics, the accuracy of hand geometry is somewhat lower but it produces a very low false reject rate.

Because hand and finger geometry have a low degree of distinctiveness, the technology is not well-suited for identification applications. Hand/finger geometry is expensive and requires some training on users and is not valid for arthritic person, since they cannot put the hand on the scanner properly. The hand/finger geometry system requires a large amount of physical space

g) Fingerprint:

Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

The fingerprint biometric method involves a user placing his finger on a platen for the fingerprint to be read. The minutiae are then extracted using a particular algorithm to create a template. Fingerprint biometrics have three main application arenas: large-scale Automated Finger Imaging Systems (AFIS) for law enforcement uses, fraud prevention in entitlement programs, and access control for facilities or computers. Fingerprints are unique to each finger of each individual and the ridge arrangement remains permanent during one's lifetime hence very high level of accuracy. In terms of cost, it is the most economical biometric user authentication technique. Fingerprint technology requires small storage space for the biometric template, reducing the size of the database memory required. Subjects have multiple fingers and in case one finger cannot be used there can be an alternative. The technology is standardized and easy to use.

Some of the disadvantages of fingerprint technology include issues of health concerns with touching a sensor used by countless individuals. The dryness or dirt of the finger can make the system make mistakes.

h) Finger Vein Biometric

Finger vein recognition is a method of biometric authentication that uses pattern-recognition techniques based on images of human finger vein patterns beneath the skin's surface and can used to identify individuals and verify their identity.

Finger vein biometric authentication system matches the vascular pattern in an individual's finger to previously obtained data. To obtain the pattern for the database record, an individual inserts a finger into an attester terminal containing a near-infrared LED (light- emitting diode) light and a monochrome CCD (charge-coupled device) camera. The hemoglobin in the blood absorbs near-infrared LED light, which makes the vein system appear as a dark pattern of lines. The camera records the image and the raw data is digitized, certified and sent to a database of registered images. For authentication purposes, the finger is scanned as before and the data is sent to the database of registered images for comparison. The authentication process takes less than two seconds.

Blood vessel patterns are unique to each individual, as are other biometric data such as fingerprints or the patterns of the iris. Unlike some biometric systems, blood vessel patterns are almost impossible to counterfeit because they are located beneath the skin's surface. Biometric systems based on fingerprints can be fooled with a dummy finger fitted with a copied fingerprint; voice and facial characteristic-based systems can be fooled by recordings and high-resolution images. The finger vein system is much harder to fool because it can only authenticate the finger of a living person. The human vascular structure is a unique & private feature of an individual and this makes finger vein technology very accurate. Another advantage is that the technology is contactless.

4.9 Proposed Authentication Prototype

Based on the facts obtained during the research on different biometric systems, the research proposed a multimodal biometric authentication prototype that uses a combination of both fingerprint and finger vein biometrics. A conceptual model for a fingerprint and finger vein authentication prototype was therefore developed. The proposed authentication prototype was to use a combination of both fingerprint and finger vein scanners but only the fingerprint scanner was readily available in the local market. The only option of getting a finger vein scanner was to import one from another country which was not possible due to the high cost involved. This hindered the researcher from developing the proposed authentication prototype. It is in this regard that a biometric authentication prototype using a fingerprint scanner only was developed. To enhance security, passwords and encryption were incorporated into the prototype.

4.9.1 Conceptual Model for a Fingerprint and Finger Vein Multimodal Prototype

The conceptual model uses two process namely, user enrollment and user authentication.

Process 1: User Enrollment

During the enrollment process the fingerprints and finger veins are extracted and their features combined. The combined extracted feature or the template is then encrypted to avoid attacks from eavesdroppers and hackers. Finally the template is registered in the database (Fig. 8). The database must be secure enough to avoid unauthorized access which could read to tampering with stored template

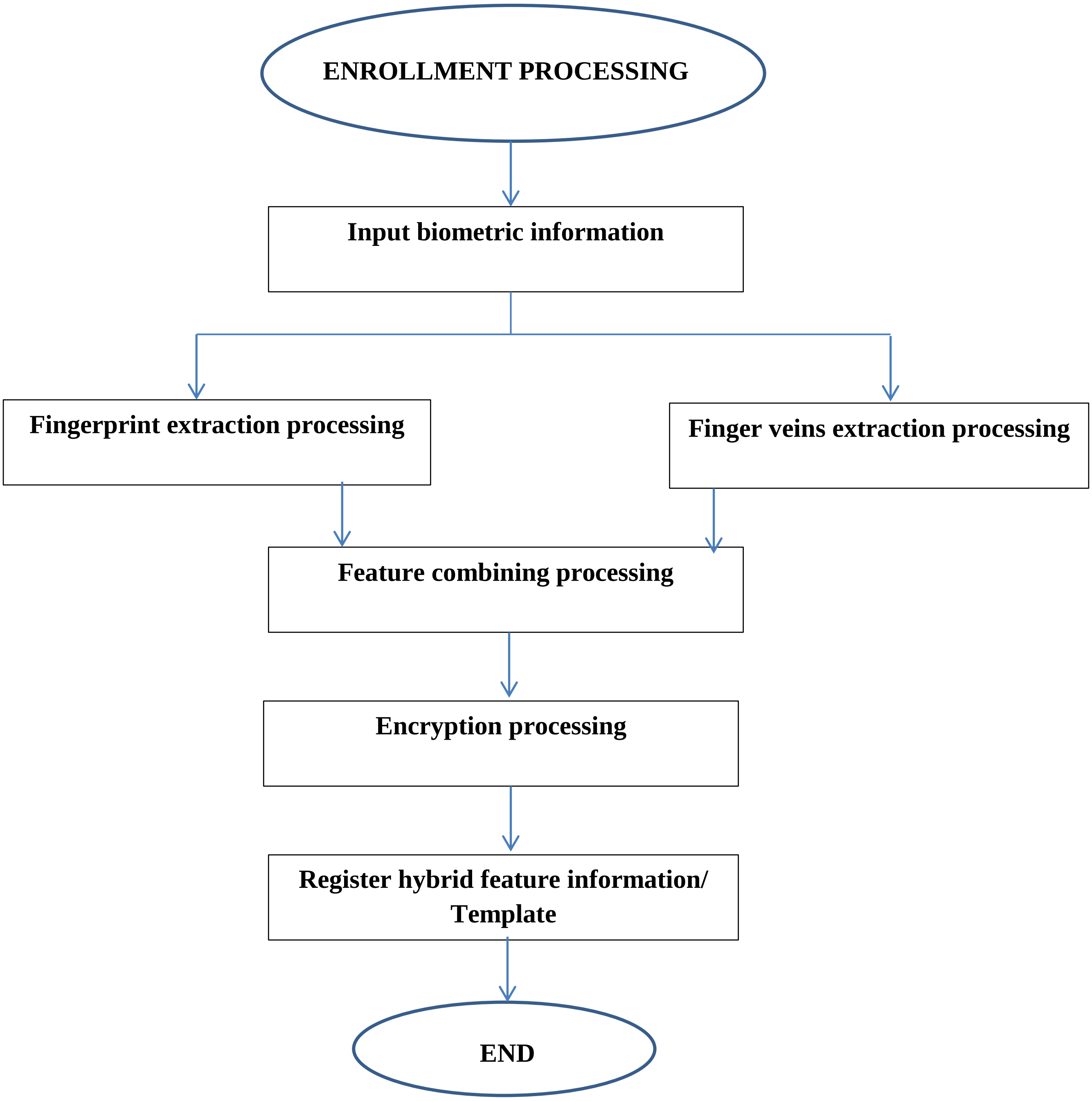

ENROLLMENT PROCESSING
Input biometric information
Fingerprint extraction processing
Finger veins extraction processing
Feature combining processing
Encryption processing
Register hybrid feature information/ Template
END

Fig. 8: User Enrollment in a Multimodal Authentication Process

Process 2: User Authentication

The second process of the conceptual model is user authentication. The fingerprint and finger veins of the user are extracted and their features combined. Fingerprint matching computation and finger vein matching computation is done and if the overall matching computation outputs a match, then the system confirms that the biometric features are of the real person and therefore he or she is allowed to transact, else he or she is denied (Fig. 9).

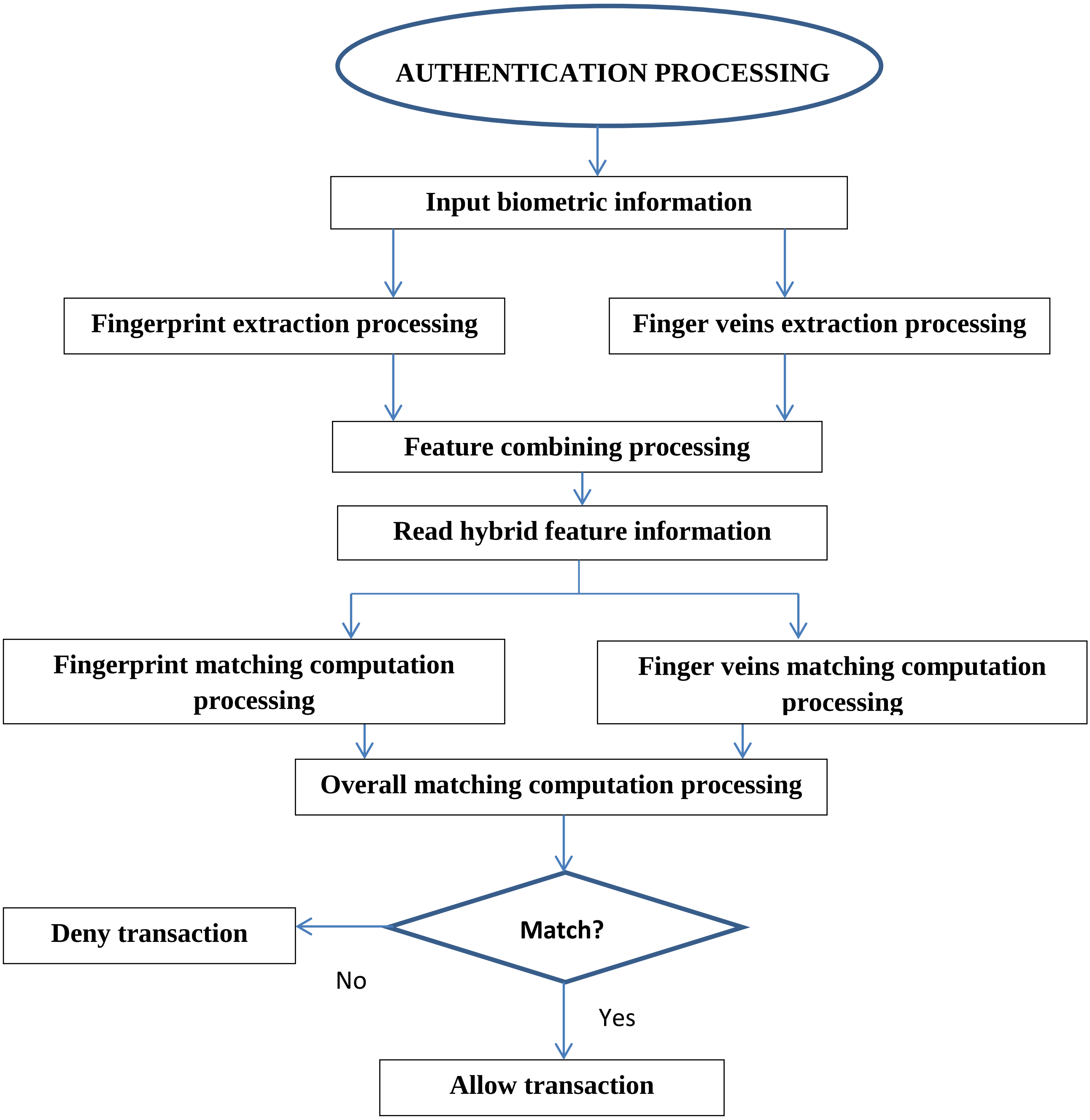

AUTHENTICATION PROCESSING
Input biometric information
Fingerprint extraction processing
Finger veins extraction processing
Feature combining processing
Read hybrid feature information
Fingerprint matching computation processing
Finger veins matching computation processing
Overall matching computation processing
Match?
Deny transaction
No
Yes
Allow transaction

Fig. 9: User Authentication in a Multimodal Authentication Process

4.10 An Illustration of how a Client can be Authenticated using the Proposed Authentication Prototype

Steps

i. Client places his registered finger on the fingerprint scanner for scanning of the fingerprints

ii. Client then places his registered finger near the finger vein reader for scanning of the finger veins

iii. The scanned fingerprints and veins are then matched with the registered templates in the database.

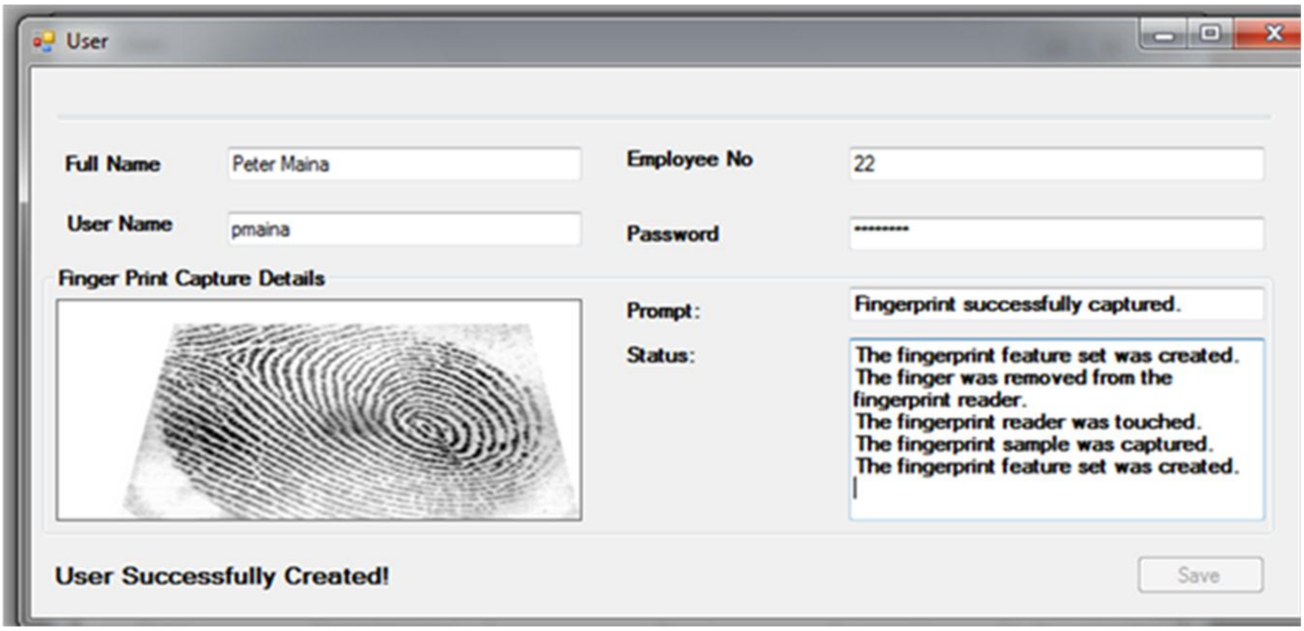
iv. If the scanned features matches with the registered ones, then this activates the client's account ready for a transaction else the account remains inactive (this means that it is only the decision of the authenticating system that can allow a transaction to happen and not the decision of the person serving you at the counter). This eradicates any chance of the person serving you at the counter being compromised. This also prevents "inside job" where an employee can do an illegal transaction on a client's account. A client's account will only became active and ready for a transaction **if and only if** the client physically presents his or her fingerprints and veins for scanning and the biometric systems confirms that they match with the registered ones.

v. Once a transaction has been executed the client's account automatically returns to inactive mode.

4.11 Some Screenshots of the Fingerprint Authentication Prototype

User Enrollment

System users who are to serve the clients are required to register their fingerprints in the system. The users have to use their fingerprints and a password to login into the system.



Full Name: Peter Maina

Employee No: 22

User Name: pmaina

Password: *********

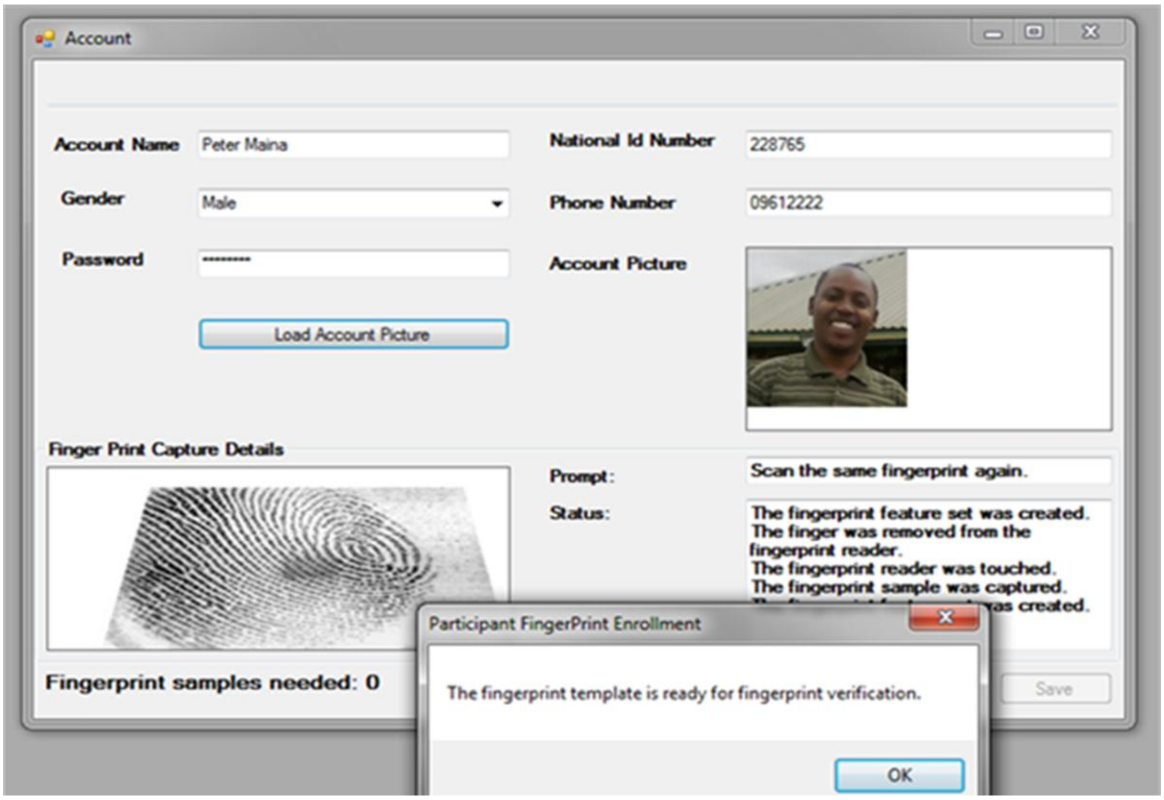
Prompt: Fingerprint successfully captured.

Status:
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.
The fingerprint reader was touched.
The fingerprint sample was captured.
The fingerprint feature set was created.

User Successfully Created!

Client Enrollment

A client is authenticated using his or her fingerprint and a password before any transaction is done


Account
Load Account Picture
Finger Print Capture Details
Save
Participant FingerPrint Enrollment
OK

Account Name: Peter Maina

National Id Number: 228765

Gender: Male

Phone Number: 09612222

Password: *********

Account Picture

Prompt: Scan the same fingerprint again.

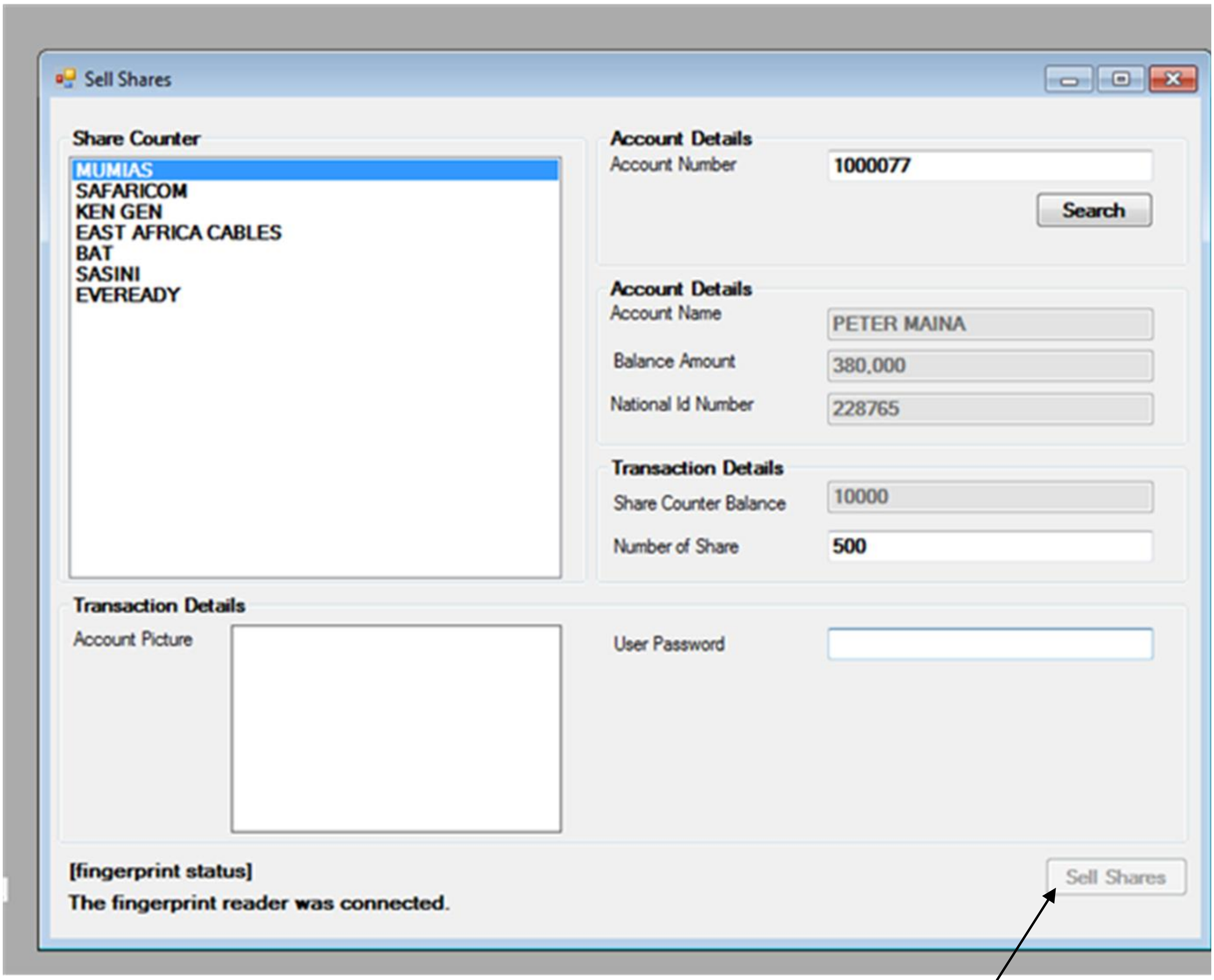
Status:
The fingerprint feature set was created.
The finger was removed from the fingerprint reader.
The fingerprint reader was touched.
The fingerprint sample was captured.
as created.

Fingerprint samples needed: 0

The fingerprint template is ready for fingerprint verification.

Selling of Shares

For a client to sell shares, he or she is required to provide the fingerprint for verification. Before the fingerprint has been verified, the client’s account remains inactive such that no transaction can be performed.



Share Counter
MUMIAS
SAFARICOM
KEN GEN
EAST AFRICA CABLES
BAT
SASINI
EVEREADY

Account Details
Account Number 1000077

Account Details
Account Name PETER MAINA
Balance Amount 380,000
National Id Number 228765

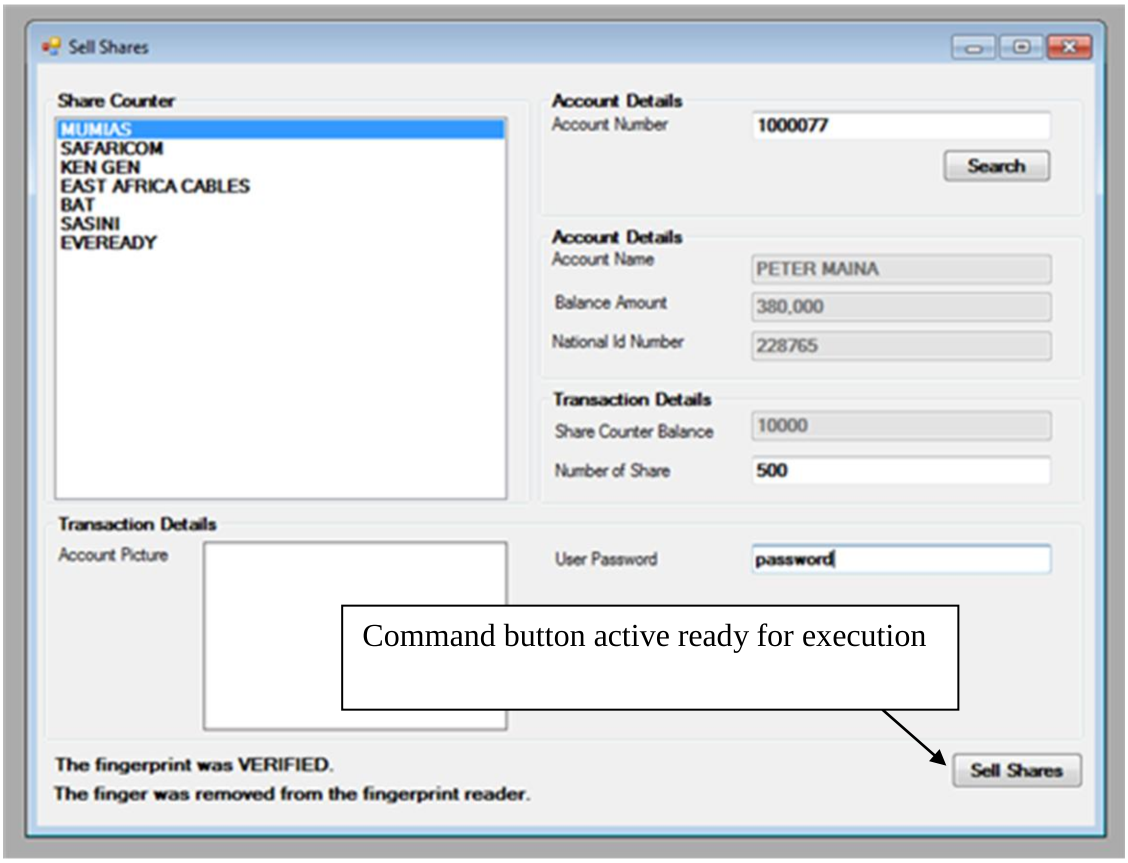
Transaction Details
Share Counter Balance 10000
Number of Share 500

Transaction Details
Account Picture
User Password

[fingerprint status]
The fingerprint reader was connected.

The command button to execute the sale of shares remains inactive until the client’s fingerprint has been verified.

After the client's fingerprint has been successfully verified, the command button for executing the sale of shares becomes active ready for a transaction.



MUMIAS
SAFARICOM
KEN GEN
EAST AFRICA CABLES
BAT
SASINI
EVEREADY

Account Number: 1000077

Account Name: PETER MAINA

Balance Amount: 380,000

National Id Number: 228765

Share Counter Balance: 10000

Number of Share: 500

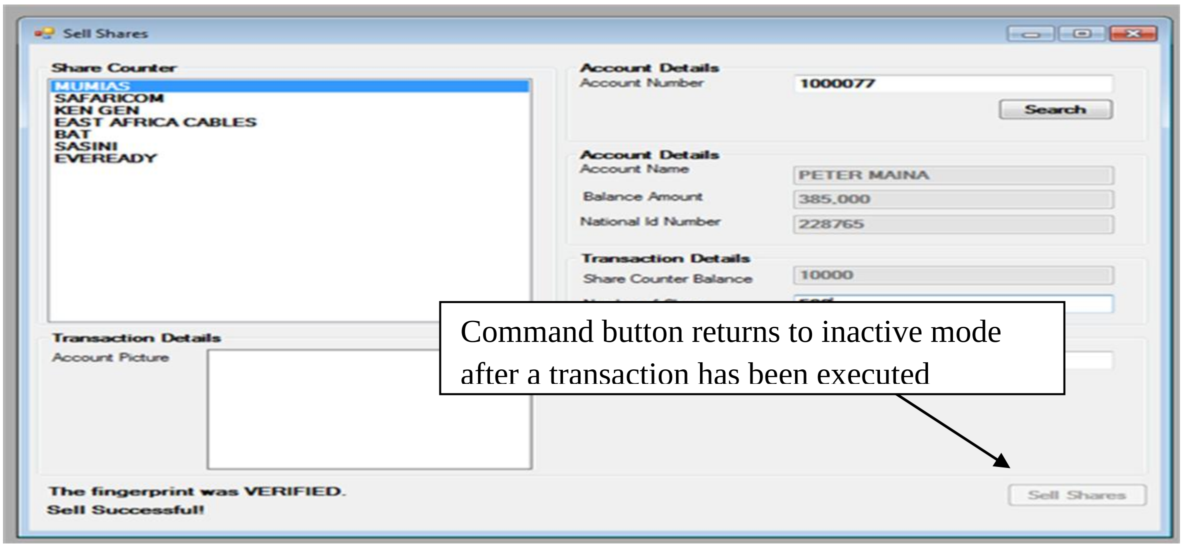
Account Picture

User Password: password

The fingerprint was VERIFIED.
The finger was removed from the fingerprint reader.

Command button active ready for execution

After the sale transaction has been executed, the command button for executing the sale of shares returns to inactive mode.



MUMIAS
SAFARICOM
KEN GEN
EAST AFRICA CABLES
BAT
SASINI
EVEREADY

Account Number: 1000077

Account Name: PETER MAINA

Balance Amount: 385,000

National Id Number: 228765

Share Counter Balance: 10000

Account Picture

The fingerprint was VERIFIED.
Sell Successful!

Command button returns to inactive mode after a transaction has been executed

4.12 Possible Areas in the Biometric Authentication Prototype that can be Prone to Attacks

During the survey, the following points of a biometric authentication were found to be vulnerable to attacks (Fig. 10).

4.12.1 Possible Types of Attacks on a Biometric Authentication

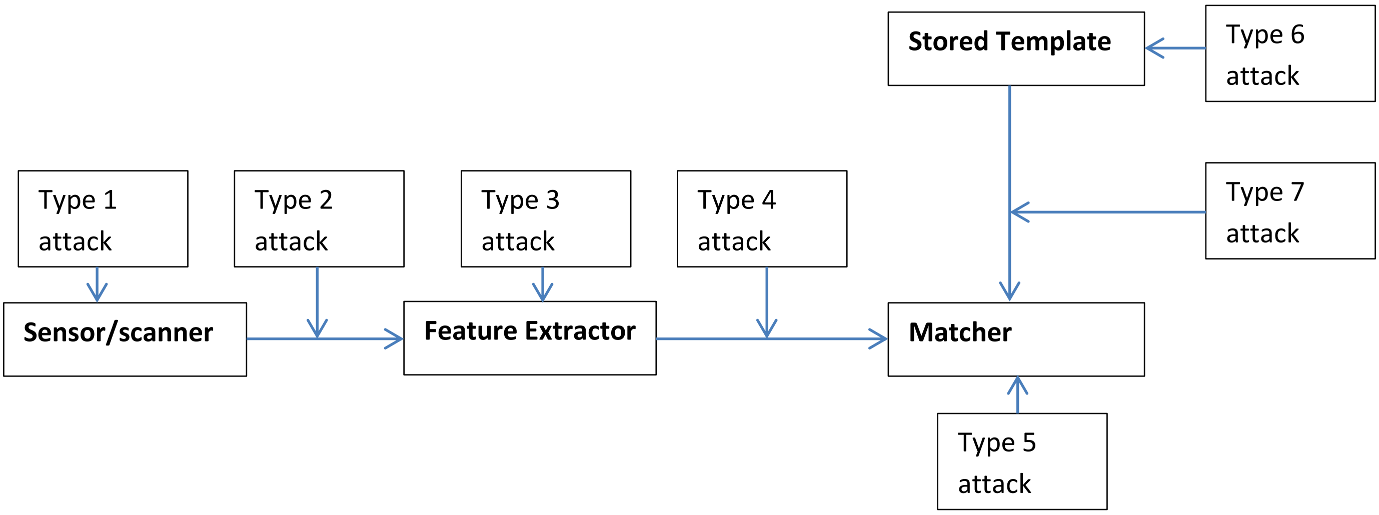


Fig. 10: Possible Attack Points on Biometric Authentication

4.12.2 Type of Possible Attacks

Type 1: **Attack at the Scanner**

This happens when a fake biometric is presented to the scanner or the scanner is physically destroyed in order to cause a denial of service.

Type 2: **Attack on the Channel between the Scanner and the Feature Extractor or "Replay Attack"**

In this attack, the attacker intercepts the communication channel between the scanner and the feature extractor to steal biometric traits and store it somewhere. The attacker can then replay the stolen biometric traits to the feature extractor to bypass the scanner.

Type 3: **Attack on the Feature Extractor Module**

In this attack, the attacker can replace the feature extractor module with a Trojan horse. Trojan horses in general can be controlled remotely. Therefore, the attacker can simply send commands to the Trojan horse to send to the matcher module feature values selected by him.

Type 4: **Attack on the Channel between the Feature Extractor and Matcher**

This attack is similar to the attack described in type 2 above. The difference is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.

Type 5: **Attack on the Matcher**

At this point the attacker replaces the matcher with a Trojan horse. The attacker can send commands to the Trojan horse to produce high matching scores and send a "yes" to the application to bypass the biometric authentication mechanism.The attacker can also send commands to the Trojan horse to produce low matching scores and send a "no" to the application all the time causing a denial of service.

Type 6: **Attack on the System Database**

In this attack, the attacker compromises the security of the database where all the templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can add new templates, modify existing templates or delete templates.

Type 7: **Attack on the Channel between the System Database and Matcher**

In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data.

4.13 Controls that can be put in Place to Avoid Attacks on the Biometric Authentication

The survey was able to identify the following ways which can be used to protect biometric data

4.13.1 Access Control

A) Physical Security

Areas where the database is stored should be physically secured in such a way that it would be very difficult for unauthorized person to get into the area. This can be achieved through the use of security doors that have biometric door locks.

B) System Access Control

The authentication system itself should also be secured from unauthorized access in order to avoid illegal manipulation of data. This can also be achieved through the use of biometrics such as fingerprint to login into the system.

4.13.2 Data Encryption

The data should be encoded in such a way that eavesdroppers or hackers cannot read it.

4.13.3 Data Backups

All important data should be copied and stored in a separate location so that it can be used in case the original data is lost or tampered with.

CHAPTER 5: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The research explored and analyzed various biometric features including the face, voice, iris, retina, DNA, fingerprint, finger vein and hand geometry. From the analysis, fingerprint and finger vein biometrics were found to be more secure, reliable and applicable in user authentication. Fingerprints and finger veins are unique and they do not change over time. The two features are also easy to capture and are less intrusive and therefore more socially acceptable.

A conceptual model of a multimodal biometric authentication was developed. The model assisted in developing a multimodal authentication prototype which used a fingerprint and a password to authenticate users. It was difficult to develop the proposed prototype which was to use fingerprint and finger vein biometrics due to lack of a finger vein scanner in the local market. The developed fingerprint and password authentication prototype was demonstrated and tested by some members of the Nairobi Securities Exchange, who recommended its performance.

Areas prone to attacks in the authentication prototype were identified and several measures were put in place to avoid and manage the attacks. Among the measures taken were data encryption and secure login in which users were required to login into the system using fingerprints.

5.2 Limitation of the Research

There were various limitations encountered during the research which included high cost of acquiring biometric devices and unavailability of some of the biometric devices in the local market. The use and knowledge of biometric authentication in Kenya is also new.

5.3 Recommendations

The research recommends that a fingerprint and finger vein multimodal authentication method should be adopted by various organizations like the stock brokerage firms and banks. To avoid unauthorized transactions, a client's account should only become active and ready for a transaction if and only if the scanned biometric features match with the registered ones in the database, else the account remains inactive (this means that it is only the decision of the authenticating system that can allow a transaction to happen and not the decision of the person serving you at the counter). This eradicates any chance of the person serving you at the counter being compromised. It also prevents inside job. Once a transaction has been executed the client's account should automatically return to inactive mode. In order to encourage the use of biometrics in Kenya, the Government should give tax incentives on biometric devices and also develop standards for the biometric devices in order to ensure compatibility, interoperability, safety, and quality of biometric devices.

5.4. Recommendations for Further Research

The research recommends a study on how biometrics can be used on mobile devices like phones such that clients can be authenticated remotely.

REFERENCES:

1. Aboalsamh, H., (2009). Vein and Fingerprint Biometrics Authentication- Future Trends. *International Journal of Computers and Communications*, Vol. 3, Issue 4.
2. Adeoye, O., (2010). Multi –Mode Biometric Solution for Examination Malpractices in Nigerian Schools. *International Journal of Computer Applications (0975 – 8887)* Vol. 4 – No.7.
3. Arunkumar,V., and Malathy, C., (2010). Multimodal Biometrics by Fusion of Finger Vein and Finger Print Images. *Proceedings of the 4th National Conference; INDIACom-2010 Computing For Nation Development*.
4. Barua, K., Bhattacharya, S., and Mali, K., (2011). Fingerprint Identification. *Global Journal of Computer Science & Technology*, Vol 11 Issue Version 1.0.
5. Bhattacharyya, D., Ranjan, R., Alisherov F., and Choi, M., (2009). Biometric Authentication: A Review. *International Journal of u- and e- Service, Science and Technology*, Vol. 2, No. 3.
6. Bhuyan, M., Saharia, S., and Bhattacharyya, D., (2010). An Effective Method for Fingerprint Classification. *International Arab Journal of e-Technology*, Vol. 1, No. 3.
7. Biometrics News Portal. What are biometrics? *(www.biometricnewsportal.com/biometrics_definition.asp).*
8. Bromba, M., Biometrics FAQ. *(http://www.bromba.com/faq/biofaqe.htm).*

9. Daily Nation, Sh500m lost to Kenya bank fraud in just a month, (http://www.nation.co.ke/News/Sh500m-lost-to-bank-fraud-in-just-a-month-/-/1056/1089298/-/a8mqlmz/-/index.html), last accessed, June 10, 2013.

10. Finger Vein/Fingerprint Sensors (http://www.morpho.com/identification/acces-securise-biometrique/capteurs-d-empreintes-digitales-et-du-reseau-veineux/?lang=en), last accessed, June 10, 2013.
11. Guillen, E., Alfonso, L., Martinez, K., and Mejia, M., (2012). Vulnerabilities and Performance Analysis over Fingerprint Biometric Authentication Network. *Proceedings of the World Congress on Engineering and Computer Science,* Vol II.
12. How do Kenyan Banks lose your money to fraudsters? (http://blog.denniskioko.com/2013/04/how-do-kenyan-banks-lose-your-money-to.html), last accessed, June 10, 2013.

13. Hybrid Finger Identification (http://www.nec.com/en/global/solutions/security/products/hybrid_finger.html) last accessed, June 10, 2013.
14. Kazi, M., Rode, Y., Dabhade S., Al-Dawla N., Mane A., Manza R., and Kale K., (2012). Multimodal Biometric System Using Face and Signature: A Score Level Fusion Approach. *Advances in Computational Research ISSN: 0975-3273 & E-ISSN: 0975-9085,* Vol. 4, Issue 1, pp.-99-103.
15. Malekinezhad, H., and Ebrahimpour, H., (2012). Protecting Biometric-based Authentication Systems against Indirect Attacks. *International Journal of Engineering Research & Technology (IJERT)* Vol. 1 Issue 6.
16. Mane, V., and Jadhav, D., (2009). Review of Multimodal Biometrics: Applications, Challenges and Research Areas. *International Journal of Biometrics and Bioinformatics (IJBB),* Vol.3, Issue 5.
17. Manivannan, N., Tigli, C., Noor, A., and Memon, S., (2011). Fingerprint Biometric for Identity management. *International Journal of Industrial Engineering and Management (IJIEM),* Vol. 2 No 2, pp. 39-44.
18. Minwei, H., Zhao, H., (2009). A Identity Authentication Based on Fingerprint Identification. *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09)*, pp. 261-263.
19. Mishra, A., (2010). Multimodal Biometrics it is: Need for Future Systems. *International Journal of Computer Applications (0975 – 8887)*Vol. 3 – No.4.
20. Nairobi Securities Exchange website. List of member firms. (http://www.nse.co.ke/member-firms/firms.html).
21. Onyesolu, M., and Ezeani, I., (2012). ATM Security Using Fingerprint Biometric Identifer: An Investigative Study. *(IJACSA) International Journal of Advanced Computer Science and Applications,* Vol. 3, No.4.
22. Razzak, M., Yusof, R., and Khalid, M., (2010). Multimodal face and finger veins biometric authentication. *Scientific Research and Essays,* Vol. 5(17), pp. 2529-2534.
23. Sasidhar, K., Kakulapati, V., Ramakrishna, K., and KailasaRao, K., (2010). Multimodal Biometric Systems - Study to Improve Accuracy and Performance. *International Journal of Computer Science & Engineering Survey (IJCSES),* Vol.1, No.2.
24. Sheeba, T., and Bernard M., (2012). Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein. *International Journal of Computer Applications (0975 – 8887)* Vol. 51– No.5.

25. Shukla, S., and Mishra, P., (2012). A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits. *International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307*, Vol.2, Issue 1.

26. Uludag, U., and Jain, A. Attacks on Biometric Systems A Case Study in Fingerprints

27. Yoshimine, T, et al., (2013). Hybrid biometric authentication device, hybrid biometric authentication method, and computer-readable medium storing hybrid biometric authentication program.(http://www.google.com/patents/US8369583), last accessed, June 10, 2013.

APPENDIX I: RESEARCH QUESTIONNAIRE

RESEARCH QUESTIONNAIRE

First, I would like to thank you in advance for taking your time to complete this questionnaire. The purpose of this questionnaire is to assist a research being carried out on" **Biometric Authentication: A case for the Nairobi Securities Exchange".** I wish to assure you that all information provided will remain confidential and will be used purely for the purpose of this Research and will not be passed on to any third party. Kindly answer the questions as truthfully as possible.

1. What is your career or role in stock exchange?

   (a) Person handling information technology/ information system's security [ ]

   (b) System's developer [ ]

   (c) Database administrator [ ]

   (d) Customer care representative [ ]

   (e) Stock holder [ ]

   (f) Any other. Please clarify…………………………………………… [ ]

2. Your gender?

   Male [ ] Female [ ]

3. Highest level of Education attained?

   Certificate/Diploma [ ] Bachelor's Degree [ ] Master's Degree [ ]

   PhD [ ]

4. Have you ever experienced or heard of someone who has lost stock to fraudulent people pretending to be the real owners of stock?

   Yes [ ] No [ ]

   If yes, how did it happen?

____

____

____

5. How does your organization verify and authenticate clients?

   Hand written signature [ ]   Identification document (National ID, Passport etc) [ ]

   Secret codes/password [ ]   Biometrics [ ]

6. Do you think the above method you have ticked is satisfactory reliable and secure?

   Yes [ ]   No [ ]

7. If the answer to question 5 above is *Biometrics* which biometric feature(s) is used?

   Fingerprint [ ]   Retina [ ]   Finger vein [ ]   Palm Vein [ ]   Face [ ]

   Iris [ ]   Any other____

8. From your own view, which combination of the above biometric features do you think could be more reliable and secure in terms of human identification and authentication?

   ____

   ____

   ____

9. What are the pro and cons of the various biometric features mentioned above?

Biometric feature	**Pros**	**Cons**
Fingerprint		
Retina		
Iris		
Face		
Palm Vein		
Finger Vein		

10. Is there a possibility that biometric data can be manipulated?

   Yes [ ]   No [ ]

   If yes, how?

____

____

____

11. Which controls can be put in place to avoid attacks on biometric authentication?

    ____

    ____

    ____

12. Is there any other challenge that may affect the successful implementation of a biometric authentication system? Yes [ ] No [ ]

    If yes, which ones?

    ____

    ____

    ____

******The End******

Thank you for taking time to complete the questionnaire

APPENDIX II: SAMPLE CODE

Sample code for creating users

```
using System;
using System.Collections;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using System.IO;
using Business;

namespace SSEAPP
{
    public partial class UIUser : Form, DPFP.Capture.EventHandler
    {
        private DPFP.Processing.Enrollment Enroller;
        private DPFP.Capture.Capture Capturer;
        private DPFP.Template Template;
        private DPFP.Verification.Verification Verificator;
        public delegate void OnTemplateEventHandler(DPFP.Template template);
        public event OnTemplateEventHandler OnTemplate;
        public string Action { get; set; }

        public UIUser()
        {
            InitializeComponent();
        }
        protected virtual void Init()
        {
            try
            {
                Capturer = new DPFP.Capture.Capture();                          // Create a capture operation.

                if (null != Capturer)
                    Capturer.EventHandler = this;                                // Subscribe for capturing
events.
                else
                    SetPrompt("Can't initiate capture operation!");
            }
            catch (Exception ex)
            {
                MessageBox.Show("Can't initiate capture operation!" + ex.Message + " (" + ex.StackTrace + ")",
"Error", MessageBoxButtons.OK, MessageBoxIcon.Error);
            }
            Enroller = new DPFP.Processing.Enrollment();
            Verificator = new DPFP.Verification.Verification();
            //this.btnSave.Enabled = false;
            UpdateStatus();
        }

        protected void Start()
        {
            if (null != Capturer)
            {
                try
                {
                    Capturer.StartCapture();
                    SetPrompt("Using the fingerprint reader, scan your fingerprint.");
                }
                catch
                {
                    SetPrompt("Can't initiate capture!");
                }
            }
        }

        protected void Stop()
        {
            if (null != Capturer)
            {
                try
                {
                    Capturer.StopCapture();
                }
                catch
                {
                    SetPrompt("Can't terminate capture!");
                }
            }
        }
        #region Form Event Handlers:
        private void UIUser_Load(object sender, EventArgs e)
        {
            Init();
            Start();
            this.btnSave.Enabled = false;
            this.lblTitle.Text = "";
            this.OnTemplate += CaptureTemplate;
        }

        private void CaptureTemplate(DPFP.Template template)
        {
            this.Invoke(new Function(delegate()
            {
                Template = template;
                if (Template != null)
                    MessageBox.Show("The fingerprint template is ready for fingerprint verification.", "Participant FingerPrint Enrollment");
                else
                    MessageBox.Show("The fingerprint template is not valid or Already Exists!", "Participant FingerPrint Enrollment");
            }));
        }

        private void UIUser_FormClosed(object sender, FormClosedEventArgs e)
        {
            Stop();
        }
        #endregion

        #region EventHandler Members:

        public void OnComplete(object Capture, string ReaderSerialNumber, DPFP.Sample Sample)
```

```
{
   MakeReport("The fingerprint sample was captured.");
   SetPrompt("Scan the same fingerprint again.");
   Process(Sample);

}

protected void Process(DPFP.Sample Sample)
{
   DrawPicture(ConvertSampleToBitmap(Sample));

   // Process the sample and create a feature set for the enrollment purpose.
   DPFP.FeatureSet features = ExtractFeatures(Sample, DPFP.Processing.DataPurpose.Enrollment);

   // Check quality of the sample and add to enroller if it's good
   if (features != null) try
      {
         MakeReport("The fingerprint feature set was created.");
         Enroller.AddFeatures(features);             // Add feature set to template.
      }
      finally
      {
         UpdateStatus();

         // Check if template has been created.
         switch (Enroller.TemplateStatus)
         {
            case DPFP.Processing.Enrollment.Status.Ready:          // report success and stop capturing
               bool exists = false;
               exists = fingerPrintExists(Sample);
               //check if fingerprint exists
               if (exists == false)
               {
                  OnTemplate(Enroller.Template);
                  SetPrompt("Fingerprint successfully captured.");
                  EnableSaveButton(true);
                  Stop();
               }
               else
               {
                  Enroller.Clear();
                  Stop();
                  UpdateStatus();
                  OnTemplate(null);
                  EnableSaveButton(false);
                  SetPrompt("Fingerprint already exists.");
                  Start();
               }
               break;

            case DPFP.Processing.Enrollment.Status.Failed:          // report failure and restart capturing
               Enroller.Clear();
               Stop();
               UpdateStatus();
               //EnableSaveButton(true);
               OnTemplate(null);
               Start();
               break;
         }
      }
```

```
        }

        private void DrawPicture(Bitmap bitmap)
        {
            this.Invoke(new Function(delegate()
            {
                Picture.Image = new Bitmap(bitmap, Picture.Size);   // fit the image into the picture box
            }));
        }

        protected Bitmap ConvertSampleToBitmap(DPFP.Sample Sample)
        {
            DPFP.Capture.SampleConversion Convertor = new DPFP.Capture.SampleConversion();    // Create a
sample convertor.
            Bitmap bitmap = null;
                                                        // TODO: the size doesn't matter
            Convertor.ConvertToPicture(Sample, ref bitmap);
                                           // TODO: return bitmap as a result
            return bitmap;
        }

        protected DPFP.FeatureSet ExtractFeatures(DPFP.Sample Sample, DPFP.Processing.DataPurpose
Purpose)
        {
            DPFP.Processing.FeatureExtraction Extractor = new DPFP.Processing.FeatureExtraction();            //
Create a feature extractor
            DPFP.Capture.CaptureFeedback feedback = DPFP.Capture.CaptureFeedback.None;
            DPFP.FeatureSet features = new DPFP.FeatureSet();
            Extractor.CreateFeatureSet(Sample, Purpose, ref feedback, ref features);                              // TODO:
return features as a result?
            if (feedback == DPFP.Capture.CaptureFeedback.Good)
                return features;
            else
                return null;
        }

        protected bool fingerPrintExists(DPFP.Sample Sample)
        {
            bool flag = false;
            // Process the sample and create a feature set for the enrollment purpose.
            DPFP.FeatureSet features = ExtractFeatures(Sample, DPFP.Processing.DataPurpose.Verification);
            // Check quality of the sample and start verification if it's good
            // TODO: move to a separate task
            if (features != null)
            {
                // Compare the feature set with our template
                foreach (DPFP.Template template in getTemplates(BaseSetting.LOGIN_BASE_PATH))
                {
                    DPFP.Verification.Verification.Result result = new DPFP.Verification.Verification.Result();
                    Verificator.Verify(features, template, ref result);
                    //UpdateStatus(result.FARAchieved);
                    if (result.Verified)
                    {
                        MakeReport("Already REGISTERED.");
                        EnableSaveButton(false);
                        flag = true;
                        continue;
                    }
                }
            }
            return flag;
        }

        public ArrayList getTemplates(string basepath)
        {
            ArrayList list = new ArrayList();
            string path = basepath;
            if (Directory.Exists(path))
            {
                Directory.CreateDirectory(path);
            }
            foreach (string filename in Directory.GetFiles(path, "*.*"))
            {
                using (FileStream fs = File.OpenRead(filename))
                {
                    DPFP.Template template = new DPFP.Template(fs);
                    list.Add(template);
                }
            }
            return list;
        }

        public void OnFingerGone(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The finger was removed from the fingerprint reader.");
        }

        public void OnFingerTouch(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The fingerprint reader was touched.");
        }

        public void OnReaderConnect(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The fingerprint reader was connected.");
        }

        public void OnReaderDisconnect(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The fingerprint reader was disconnected.");
        }

        public void OnSampleQuality(object Capture, string ReaderSerialNumber,
    DPFP.Capture.CaptureFeedback CaptureFeedback)
        {
            if (CaptureFeedback == DPFP.Capture.CaptureFeedback.Good)
                MakeReport("The quality of the fingerprint sample is good.");
            else
                MakeReport("The quality of the fingerprint sample is poor.");
        }
        #endregion

        protected void SetStatus(string status)
        {
            this.Invoke(new Function(delegate()
            {
                StatusLine.Text = status;
            }));
        }
        protected void SetPrompt(string prompt)
        {
            this.Invoke(new Function(delegate()
            {
                Prompt.Text = prompt;
            }));
        }
        protected void EnableSaveButton(bool flag)
        {
            this.Invoke(new Function(delegate()
            {
                this.btnSave.Enabled = flag;
            }));
        }

        protected void MakeReport(string message)
        {
            this.Invoke(new Function(delegate()
            {
                StatusText.AppendText(message + "\r\n");
            }));
        }

        private void UpdateStatus()
        {
            // Show number of samples needed.
            SetStatus(String.Format("Fingerprint samples needed: {0}", Enroller.FeaturesNeeded));
        }

        private void btnSave_Click(object sender, EventArgs e)
        {
            try
            {
                SystemUser systemuser = getSystemUser();
                string filename = Path.Combine(BaseSetting.LOGIN_BASE_PATH,
systemuser.FingerPrintTemplateName);
                using (FileStream fs = new FileStream(filename, FileMode.Create, FileAccess.Write))
                {
                    systemuser.FingerPrintTemplate.Serialize(fs);
                }
                SystemUserController.createSystemUser(systemuser);
                StatusLine.Text = "User Successfully Created!";
            }
            catch (Exception ex)
            {
                StatusLine.Text = "Error occured during User Creation!";
            }
            finally
            {
                Stop();
                this.btnSave.Enabled = false;
            }

        }

        private SystemUser getSystemUser()
        {
            SystemUser systemuser = new SystemUser();
            systemuser.UserName = txtUserName.Text;
            systemuser.Password = txtPassword.Text;
            systemuser.Name = txtFullName.Text;
            systemuser.EmployeeNo = txtEmployeeNo.Text;
            systemuser.FingerPrintTemplate = this.Template;
            systemuser.FingerPrintTemplateName = Guid.NewGuid().ToString("N").ToUpper();
            return systemuser;
        }
    }
}
```

Sample code for selling shares

```
using System;
using System.Collections;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Threading.Tasks;
using System.Windows.Forms;
using SSEAPP;
using Business;
using System.IO;

namespace SSEAPP
{
    public partial class UISellShares : Form, DPFP.Capture.EventHandler
    {
        private Account Account { get; set; }
        private ShareAccount ShareAccount { get; set; }
        private DPFP.Verification.Verification Verificator;
        private DPFP.Capture.Capture Capturer;
        private string FingerPrintBasePath { get; set; }

        public UISellShares()
        {
            InitializeComponent();
            loadDefaults();
        }
        public void loadDefaults()
        {
            loadShareCounterPrice();
            loadControlDefaults();
        }
        public void loadControlDefaults()
        {
            this.btnSellShares.Enabled = false;
            txtShareCounterBalance.Text = null;
        }

        public void loadShareCounterPrice()
        {
            lbxShareCounter.DataSource = ShareCounterController.getShareCounters();
            lbxShareCounter.DisplayMember = "Name";
            lbxShareCounter.ValueMember = "Id";
            //selectShareCounter();
        }
        public void setShareBalance()
        {
            if (lbxShareCounter.SelectedValue != null)
            {
                string sharecounterid = lbxShareCounter.SelectedValue.ToString();
                if (this.Account != null)
                {
                    ShareAccount shareaccount = ShareAccountController.getShareAccount(this.Account.Id,
sharecounterid);
                    this.txtShareCounterBalance.Text = shareaccount.NumberOfShares.ToString();
                }
            }
        }

        //public void selectShareCounter()
        //{
        //    if (lbxShareCounter.SelectedIndex >= 0 && lbxShareCounter.Items.Count > 0)
        //    {
        //        ShareCounter sharecounter = (ShareCounter)lbxShareCounter.SelectedItem;
        //        txtShareCounterName.Text = sharecounter.Name;
        //        txtShareCounterNoOfShare.Text = sharecounter.NumberOfShares.ToString();
        //        txtShareCounterPrice.Text = sharecounter.SharePrice.ToString();
        //    }
        //}
        private void UISellShares_FormClosed(object sender, FormClosedEventArgs e)
        {
            Stop();
        }
        #region FingerPrint
        protected void MakeReport(string message)
        {
            this.Invoke(new Function(delegate()
            {
                lblStatus.Text = message;
            }));
        }

        protected void verifyFingerPrint(DPFP.Sample Sample)
        {
            // Process the sample and create a feature set for the enrollment purpose.
            DPFP.FeatureSet features = ExtractFeatures(Sample, DPFP.Processing.DataPurpose.Verification);
            // Check quality of the sample and start verification if it's good
            // TODO: move to a separate task
            bool matchflag = false;
            try
            {
                if (features != null)
                {
                    // Compare the feature set with our template
                    //get officer
                    string filename = Path.Combine(BaseSetting.BASE_PATH, Account.FingerPrintTemplateName);
                    DPFP.Template template = getTemplateFromFilePath(filename);
                    DPFP.Verification.Verification.Result result = new DPFP.Verification.Verification.Result();
                    Verificator.Verify(features, template, ref result);
                    //UpdateStatus(result.FARAchieved);
                    if (result.Verified)
                    {
                        VerificationReport("The fingerprint was VERIFIED.");
                        matchflag = true;
                    }
                    if (matchflag == true)
                    {
                        VerificationReport("The fingerprint was VERIFIED.");
                        EnableRegisterButton(true);
                    }
                    else
                    {
                        EnableRegisterButton(false);
                        VerificationReport("The fingerprint was NOT VERIFIED.");
                    }
                }
            }
            catch (Exception ex)
            {
            }
        }

        protected void VerificationReport(string message)
        {
            this.Invoke(new Function(delegate()
            {
                lblFingerPrintStatus.Text = message;
            }));
        }

        private void EnableRegisterButton(bool flag)
        {
            this.Invoke(new Function(delegate()
            {

                btnSellShares.Enabled = flag;
            }));
        }

        protected DPFP.FeatureSet ExtractFeatures(DPFP.Sample Sample, DPFP.Processing.DataPurpose Purpose)
        {
            DPFP.Processing.FeatureExtraction Extractor = new DPFP.Processing.FeatureExtraction();            // Create a feature extractor
            DPFP.Capture.CaptureFeedback feedback = DPFP.Capture.CaptureFeedback.None;
            DPFP.FeatureSet features = new DPFP.FeatureSet();
            Extractor.CreateFeatureSet(Sample, Purpose, ref feedback, ref features);                            // TODO: return features as a result?
            if (feedback == DPFP.Capture.CaptureFeedback.Good)
                return features;
            else
                return null;
        }

        private DPFP.Template getTemplateFromFilePath(string filepath)
        {
            DPFP.Template template = null;
            using (FileStream fs = File.OpenRead(filepath))
            {
                template = new DPFP.Template(fs);
            }
            return template;
        }
```

```
    protected virtual void Init()
    {
      try
      {
        Capturer = new DPFP.Capture.Capture();                    // Create a capture operation.

        if (null != Capturer)
          Capturer.EventHandler = this;                           // Subscribe for capturing
events.
        else
          MessageBox.Show("Can't initiate capture operation!");
      }
      catch
      {
        MessageBox.Show("Can't initiate capture operation!", "Error", MessageBoxButtons.OK,
MessageBoxIcon.Error);
      }
      Verificator = new DPFP.Verification.Verification();
    }

    protected void Start()
    {
      if (null != Capturer)
      {
        try
        {
          Capturer.StartCapture();
        }
        catch
        {
          MessageBox.Show("Can't initiate capture!");
        }
      }
    }

    protected void Stop()
    {
      if (null != Capturer)
      {
        try
        {
          Capturer.StopCapture();
        }
        catch
        {
          MessageBox.Show("Can't terminate capture!");
        }
      }
    }

    #region EventHandler Members:

    public void OnComplete(object Capture, string ReaderSerialNumber, DPFP.Sample Sample)
    {
      MakeReport("The fingerprint sample was captured.");
      verifyFingerPrint(Sample);
    }

    public void OnFingerGone(object Capture, string ReaderSerialNumber)
```

```
        {
            MakeReport("The finger was removed from the fingerprint reader.");
        }

        public void OnFingerTouch(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The fingerprint reader was touched.");
        }

        public void OnReaderConnect(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The fingerprint reader was connected.");
        }

        public void OnReaderDisconnect(object Capture, string ReaderSerialNumber)
        {
            MakeReport("The fingerprint reader was disconnected.");
        }

        public void OnSampleQuality(object Capture, string ReaderSerialNumber,
DPFP.Capture.CaptureFeedback CaptureFeedback)
        {
            if (CaptureFeedback == DPFP.Capture.CaptureFeedback.Good)
                MakeReport("The quality of the fingerprint sample is good.");
            else
                MakeReport("The quality of the fingerprint sample is poor.");
        }
        #endregion
        #endregion

        private void lbxShareCounter_Click(object sender, EventArgs e)
        {
            //selectShareCounter();
        }

        private void btnSearch_Click(object sender, EventArgs e)
        {
            string sharecounterid = ((ShareCounter)lbxShareCounter.SelectedItem).Id;
            Account account = AccountController.getAccountByAccountNo(txtAccountNumber.Text);
            ShareAccount shareaccount = ShareAccountController.getShareAccount(account.Id, sharecounterid);
            btnSellShares.Enabled = false;
            this.txtShareCounterBalance.Text = null;
            if (account != null)
            {
                this.Account = account;
                this.ShareAccount = shareaccount;
                txtAccountName.Text = account.Name;
                txtNationalId.Text = account.NationalIdNumber;
                txtAmount.Text = account.ActiveBalanceAmount.ToString("#,##0.##");
                if (shareaccount != null)
                {
                    txtShareCounterBalance.Text = shareaccount.NumberOfShares.ToString();
                }
                lblSearchDetails.Text = "";
                lblStatus.Text = null;
                Init();
                Start();
            }
            else
            {
                this.Account = null;
                this.ShareAccount = null;
                txtAccountName.Text = null;
                txtNationalId.Text = null;
                txtAmount.Text = null;
                lblSearchDetails.Text = "No Such Account Number!";
                this.btnSellShares.Enabled = false;
                txtShareCounterBalance.Text = null;
                lblStatus.Text = null;
            }
        }

        private ShareTransaction getShareTransaction()
        {
            ShareTransaction sharetransaction = new ShareTransaction();
            if (this.Account != null)
            {
                sharetransaction.AccountId = this.Account.Id;
                sharetransaction.ShareCounterId = lbxShareCounter.SelectedValue.ToString();
                int shares = 0;
                bool flag = int.TryParse(txtNoOfSharesToBuy.Text, out shares);
                sharetransaction.NumberOfShares = shares;
                ShareCounter sharecounter =
ShareCounterController.getShareCounter(sharetransaction.ShareCounterId);
                sharetransaction.Amount = sharecounter.SharePrice * sharetransaction.NumberOfShares;
            }
            else
            {
                sharetransaction = null;
            }
            return sharetransaction;
        }

        private void btnSellShares_Click(object sender, EventArgs e)
        {
            btnSellShares.Enabled = false;
            ShareTransaction sharetransaction = getShareTransaction();
            ShareCounter sharecounter =
ShareCounterController.getShareCounter(sharetransaction.ShareCounterId);
            ShareAccount shareaccount = ShareAccountController.getShareAccount(this.Account.Id,
sharetransaction.ShareCounterId);
            if (shareaccount.NumberOfShares < sharetransaction.NumberOfShares)
            {
                lblStatus.Text = "Cannot Sell More Shares than you have!";
                return;
            }
            sharetransaction = ShareTransactionController.sellShareTransaction(sharetransaction);
            if (sharetransaction != null)
            {
                Account account = AccountController.getAccount(this.Account.Id);
                this.Account = account;
                txtAmount.Text = this.Account.ActiveBalanceAmount.ToString("#,##0.##");
                lblStatus.Text = "Sell Successful!";
            }
            else
            {
                lblStatus.Text = "Unsuccessful Sell. Error Occurred!";
            }
            //Stop();
        }
        private void lbxShareCounter_SelectedIndexChanged(object sender, EventArgs e)
        {
            this.txtShareCounterBalance.Text = null;
            string sharecounterid = ((ShareCounter)lbxShareCounter.SelectedItem).Id;
            if (this.Account != null)
            {
                ShareAccount shareaccount = ShareAccountController.getShareAccount(this.Account.Id,
sharecounterid);
                this.ShareAccount = shareaccount;
                if (shareaccount != null)
                {
                    this.txtShareCounterBalance.Text = shareaccount.NumberOfShares.ToString();
                }
            }
        }
    }
}
```