UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING AND INFORMATICS

A model of Two-Factor Authentication using Facial Recognition in Automated Teller machines

Presented By:

KAMAU DAVID BIARU

REG NO: P58/75646/2012

Supervisor: Dr. Lawrence Muchemi

November 2014

A Project submitted in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science

Declaration

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

Signed:…… Date:…..……..…

KAMAU DAVID BIARU.

P58/75646/2012

This project has been submitted as a partial fulfillment of the requirements for a Master of Science Degree in Computer Science in the University of Nairobi with my approval as the university supervisor.

Signed: …….. Date: ……

DR. LAWRENCE MUCHEMI.

Abstract

The general idea of this research work is to use facial recognition technique to reinforce security on Automatic Teller Machines. The use of face recognition is to authenticate an individual by identifying and verifying him/her in an existing and up –to-date database of peoples face images. The level of security in ATM's has changed tremendously since their introduction in the late 70's. This has caused them to be very vulnerable because technology has brought in a new kind of attackers who have been using the advancement of technology to compromise their security. Something has to be done to guarantee security when it comes to people's funds and other confidential information.

Face recognition is a technique that uses application software to determine the identity of an individual and is within the category of biometrics which is defined as "the automatic recognition of a person using distinguishing traits" (RAND, 2003). Face recognition is among other biometrics including iris recognition, fingerprint, hand print and retina scans. This research provides a review of face-based authentication in accessing critical and confidential information in computer systems, the underlying motivation being to provide the latest review of the existing literature on facial recognition and to bring to the limelight, the studies of computer vision in recognition of human faces. In order to provide a comprehensive review, we have provided detailed descriptions of representative methods and related topics such as issues of (lighting) illumination and pose variation.

Keywords*: Identification, Verification, Face Recognition, Biometrics, false rejection, false acceptance*

Acknowledgement

Projects are successful because of the effort and dedication of a number of people around you who have given a helping hand and sound advice. I appreciate all those who have made this project a success through support, guidance and inspiration.

Am extremely grateful for the confidence and trust bestowed in me for my project entitled 'A model of Two-Factor Authentication using Password and Facial Recognition in Banking Applications' with special reference to University of Nairobi.

I express my sincere gratitude to Dr. Lawrence Muchemi for making effort, guidance and providing valuable insights that have led to the successful completion of my final year project.

I also express my gratitude to Prof Timothy Waema, Dr Elisha Abade and Dr Dan Orwa for giving me guidance and encouragement during project presentation and the motivation to keep on and the entire faulty for their helpful advice and provision of resources without which my project would not have been possible.

Many thanks to my family members and friends for being my source of encouragement during the entire preparation of my project work.

I thank God for His grace that has seen me through from the start up to the end of this project preparation.

Dedication

I dedicate this project to my parents Kamau D. Biaru and Rose Muthoni Kamau for their encouragement, motivation and advice.

Table of contents

List of figures

List of tables

List of abbreviations

EBGM — Elastic Bunch Graph Matching

EER — Equal Error Rate

FAR — False Accept Rate

FERET — The Face Recognition Technology program

FRGC —Face Recognition Grand Challenge

FRR — False Reject Rate

FRS — Face/Facial Recognition System

PCA — Principal Component Analysis

SVM — Support Vector Machines

TAR — True Accept Rate

TRR — True Reject Rate

FRVT — Face Recognition Vendor Test

1.0 INTRODUCTION

Normally, human beings use faces to distinguish between individuals and current advancements in computer vision capability within the last few years have enabled similar recognitions automatically. Traditional face recognition algorithms used simple geometric models, which have progressively matured over the years into a science of complex mathematical models and representations, thus drawing face recognition technology into the limelight for both verification and identification purposes. Verification is the process of comparing one biometric patterning with another biometric pattern, resulting in either a rejection or acceptance decision, (Heseltine, 2005). Identification is the process of comparing one biometric pattern with a set of two or more biometric patterns in order to determine the most likely match, (Heseltine, 2005).

Authentication in computer information systems has been by tradition based on something that one has for example magnetic strip cards, smart cards or even keys, or what one knows for example usernames and passwords, PIN or other secret codes. In order for more reliability in verification or identification processes to be achieved, something that uniquely identifies and characterizes a given person should be adopted, and biometrics technology offers computerized methods of identity verification using the concept of measurable physiological or behavioral characteristics for instance iris, retinal or face sample. These characteristics are often referred to as bio-data and must be measurable and unique.

This paper presents my findings of facial recognition, a subset of biometric authentication techniques and its deployment possibility in banking applications. Our research work and model will help companies and individuals consider the use of facial recognition as an authentication mechanism in various computer systems and networks.

1.1 ATMs and authentication of ATMs

An ATM is an electronic banking outlet that enables clients to complete basic monetary transactions without the help of a branch representative or teller (Merriam-Webster). Customers are able to perform various banking operations, such as cash withdrawal, deposits, payment of bills, obtaining bank statements and effecting cash transfers among other transactions.

ATMs basically cash withdrawal and account's balance statements. The more complex machines will accept deposits; facilitate credit card payments and report account information (Business Dictionary).

1.1.1 Knowledge: Something only the user knows

In this case, the user is required to prove knowledge of a secret in order to be authenticated.

Password: A password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user (Margaret Rouse, 2005). However, there is a growing body of evidence that people cannot cope with the password policies imposed on them (Sasse et al, 1999), and this has posed as the biggest drawback of passwords as a tool of authentication, given the choice users choose the weakest password they can get away with (Herley, 2007).

PIN: A numerical code used in many electronic financial transactions (Investopedia). It stands for Personal Identification Number and is typically used in ATMs. PINs are usually used in conjunction with usernames or other passwords. They are also usually required when using bank debit or credit cards, and most banks or financial institutions issue PINs separately from the cards through the mail. However, it has been found to be open to a form of cloning, despite past assurances from banks that chip and pin could not be compromised. 'We've never claimed that chip and pin is 100% secure and the industry has successfully adopted a multi-layered approach to detecting any newly-identified types of fraud" (Samzenpus, 2012)

Pattern: Pattern factor is a sequence or array of sets of information as e.g. automatically detectable and processible coding. It is used for authenticating the users e.g. pattern factor based authentication is used by the bearer presented to a sensor unit to get authenticated by a processing unit.

Security patterns are an agreed upon method to describe best practice solutions for common security problems (Schumacher, 2005).

1.1.2 Ownership: Something only the user has

A possession may be a physical device given to an authorized user for authentication. Examples include hardware token, USB token or software token.

1.1.3 Biometrics: Something only the user is

This is the automatic recognition of a person using distinguishing traits (RAND, 2003). Face recognition is among other biometrics including iris recognition, fingerprint, hand print and retina scans.

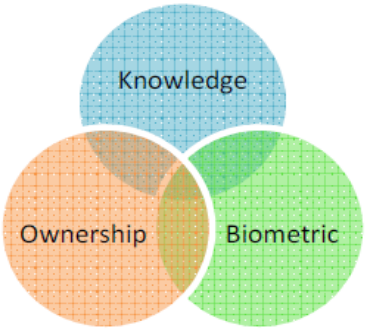


Figure 1.1: Modes of authentication of ATMs

1.2 Current practices in ATMs

The Procedure to get money from a normal standard ATM can be described as followed:

1. Customer inserts Card (for identification)
2. Customer enters PIN number (for verification)
3. ATM sends data to a central bank
4. ATM offers access to financial services

The standard ATM system uses a two level authentication:

1. Identification: to identify the customer

   A **one** to **many**

2. Verification: to ensure that the identified user is using the system

   A **one** to **one**

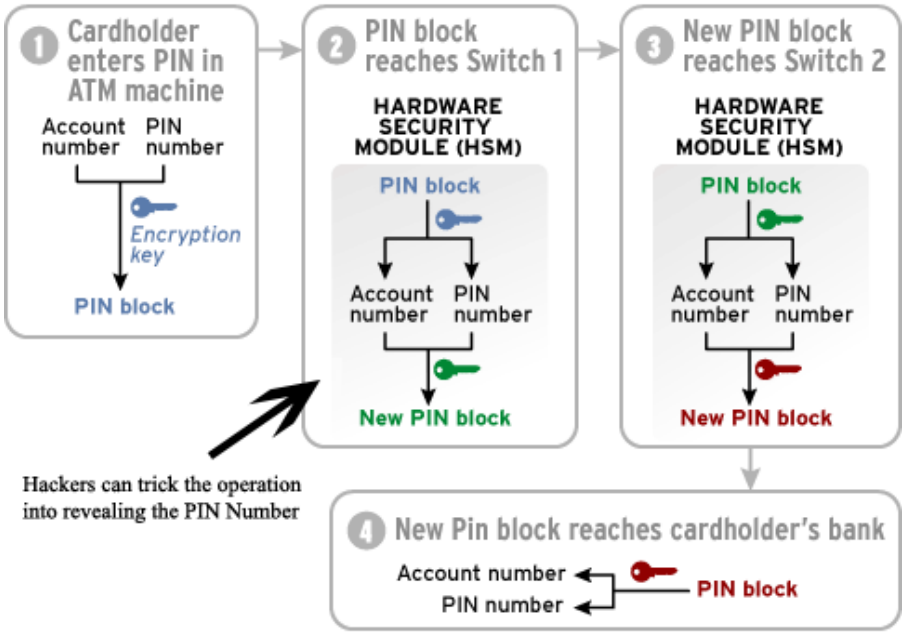


Figure 1.2: Standard ATM security framework

1.3 A study on the trend of authentication in ATMs

For enterprises that haven't revisited their authentication strategies in several years, it may be time to take a fresh look. According to Gartner Inc., a confluence of technology trends affecting enterprises such as mobility, social media, cloud computing and big data are having an effect on virtually every area of IT, including the market for enterprise authentication technology. It is inevitable to adopt two-factor authentication in one form or another.

Personal identification number (PIN)

The user is expected to provide a user identifier/token such as a card and a PIN to be authorized to access the system. When the system receives the Client ID and PIN, it compares the stored credentials with the received data. Access is granted only when there is a match between the captured details and the ones stored in the system. PINs are the most often used authentication mechanisms for ATMs.

PIN Length

At first, Shepherd-Barron envisioned a six-digit PIN number, but his wife nonetheless preferred four digits, which became the standard PIN length for all vending and ATM machines.

Password

The user presents a valid identity (ID Number) and a password to access the account. A password should be kept secret and should also be short enough to be memorized. They can be digits, letters or alphanumeric codes. The use of passwords is known to be ancient.

Smart cards

Are defined as any pocket-sized card with embedded integrated circuits which can process information (smartcard alliance, 2009) It has a microchip embedded in it which makes it “smart” and that allows other devices to communicate with it. The processing power of smart cards gives them the versatility needed to make payments, to configure your cell phones and connect to your computers via satellite or the internet (Guthery & Scott, 2001).

Biometrics

Biometrics offers the best solution for increased security requirements of information systems than passwords, PIN, and cards with PIN number.

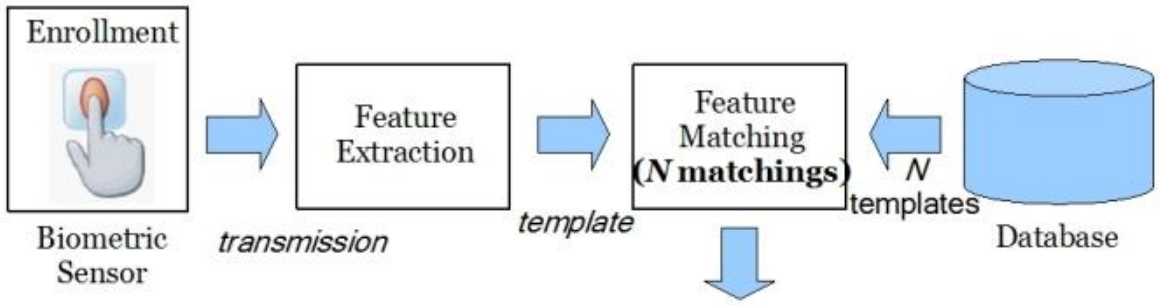
Some of the characteristics that make biometrics a better solution include:

1. The person to be identified must be physically present during identification,

2. It averts the need for the person to remember a password, PIN or carry a card.

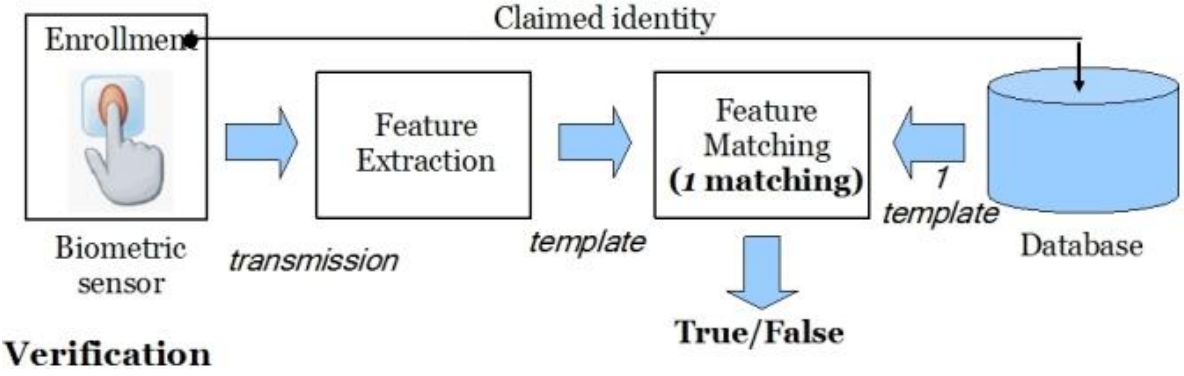
1.4 Research within password and biometrics authentication in ATMs

It is defined as the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences (Adigun et al, 2014). It may also be referred to the technique for measuring and analyzing a person's physiological or behavioral characteristics, such as retina, DNA, fingerprint, gait, face and voice for identification and verification purposes.



Identification

Figure 1.3a: Biometric system (Identification)



Verification

Figure 1.3b: Biometric system (Verification)

This diagram above represents a block diagram of a general biometric system. Several biometric systems networked together with telecommunications technology form a telebiometric system. It is distributed in nature with semi-autonomous terminals that do the identification and verification purposes. These thermals are responsible for both enrolment and test operations. In the enrolment phase, a person`s biometric information is captured and stored in a database. In the test phase, real-time biometric information is detected, captured and compared with the one

stored in the database. It should be noted that the security of the storage and retrieval operations of such systems should be secure especially if the system is to be non-intrusive.

1. Sensor: it acquires biometric information from a person.
2. Pre-processor: it performs all the necessary pre-processing i.e. removing noise
3. Extractor: extracts features from the image.

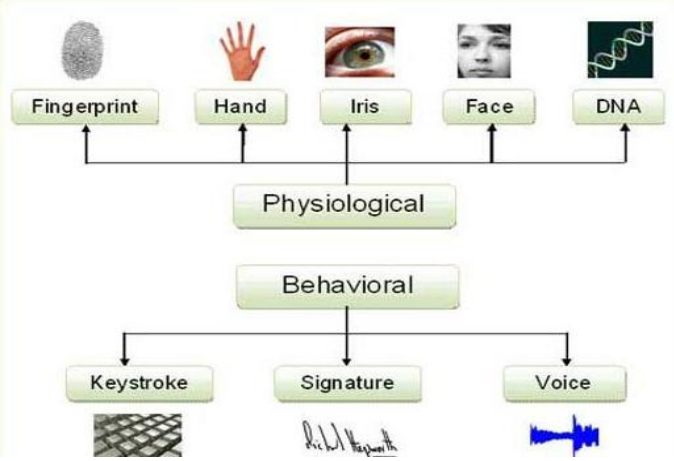


Figure 1.4: Classification of biometrics

Physiological characteristics: relates to the shape of the body e.g.:

1. Bertillonage: - relates to measuring the body lengths. (it is obsolete);
2. Finger print:- relates to analyzing fingerprint patterns;
3. Facial recognition: – relates to measuring face attributes;
4. Hand geometry: – relates to measuring the shape of the hand;
5. Iris scan: – deals with analyzing the features of colored ring of the eye;
6. Retinal scan: – deals with analyzing vein patterns;
7. DNA – involves analyzing genetic makeup of a human being.

Behavioral characteristics: relates to the behavior of a person e.g.:

1. Voice recognition: – involves analyzing the vocal behavior;
2. Signature verification: – involves analyzing signature dynamics;
3. Keystroke dynamics: – involves measuring the time spacing of typed words.

Password

Password is the most used method of restricting access to computer system accounts. Usually, the user presents a valid ID and a password to use the account. Most systems print dots or asterisk instead of the real characters.

Passwords are prone to cracking. This is done by getting a copy of the 1-way hash code in the database, and then using the appropriate algorithm to decode until a match is found.

The most appropriate method of countering password cracking is ensuring that attackers do not even get access to the encrypted password in the server.

1.5 Attaining a Two-factor authentication model

After identification of the requirements and scope of ATM security, we discussed how to integrate our facial recognition component in the ATM architecture.

According to figure 16 above, user plane is the plane that directly interacts with user. Therefore to meet the user's security objectives, user plane has to provide security services like access control, authentication, data confidentiality and integrity.

1.6 Problem statement

ATM machines face a lot of threats due to the fact that they are public utilities and that there are no measures to control who accesses them at any one point in time. There is lack of a formal model to guarantee security using biometrics technology and to describe secure software system architecture with a stepwise refinement methodology. The methodology for system modelling and refinement specifies a set of architectural and operational components and how they interact with each other.

This is why we are interested in developing a two-factor authentication mechanism using a second factor authentication which is "something that is part of the user".

Human behavioral patterns (gait, handwriting, keystroke, voice, etc) fluctuate due to anxiety, exhaustion, or sickness. However, the physiological methods (retina, face, iris, fingerprint, palm, etc) are more stable than methods in the behavioral category, the reason being that physiological features are often non-alterable except by severe injury and have the benefit of non-intrusiveness. Facial recognition is the primary focus in this study.

1.7 Goal of the study

Use facial recognition technique that will help in the development and training of a learning component which through learning will train an application. Specifically, seeking to use the concept of a learning algorithm to absorb user characteristic features of a face and then use them for authentication. This algorithm will be combined with the face recognition technique to provide non-intrusive security machinery for ATM`s.

1.8 Objectives

The objectives of this research project are:

- Carry out a survey of various authentication models for Automated Teller Machines;
- Design and develop an authentication model that uses two-factors i.e. biometrics and password authentication;
- Simulate the two-factor model and evaluate its performance;
- Demonstrate the practicality of the facial recognition component.

1.9 Justification of the study

Application software designers are spending a lot of resources and techniques in trying to develop systems with enhanced security features to prevent access by unauthorized users. Fixing of security loop holes exploited by disgruntled users may take long to be fixed or upgraded with patches. Adding a security feature that allows access based on who you are and that you are who you claim to be will keep off attackers since face recognition is non-intrusive and cannot be fooled by images.

1.10 Scope of the study

This study focuses on the addition of a facial recognition component on top of the PIN-based approach being used in the current ATM system.

2.0 LITEREATURE REVIEW

2.1 Introduction

This section will investigate into some of the literature on face recognition. Attempts to automate face recognition began in the 1960s with the initial work of Bledsoe, 1964 even though the first functional implementation of automation of face recognition is owed to Kanade, 1977. Research on automation of face recognition has since then focused on 2 dimensional images with less attention to what 3 dimensional data could offer.

2.2 Background

The attempt to automate face identification using computers is relatively a new concept that is being explored by computer scientists. The first model of facial recognition that semi automated the process was developed in the 1960s, (Turk et al, 1991) and required the user to locate the principle components including the eyes, nose, mouth and ears on the images and calculating the distances and ratios to a given point of reference, which would then be compared to some predefined data.

Harmon et al, 1970 used specified components such as the eyebrow ridge, the hair color and the thickness of the lips to automatically recognize faces, but encountered the problem of measuring the components and defining their locations because they were calculated manually. This led to the failure of these two early solutions to computerizing facial recognition.

In 1988, Sirovich and Kirby, attempted to use eigenfaces algorithm as an approach to automation with a study of the low-end two-dimensional representation of face images. They showed that PCA could be applied on a set of face images to extract a set of features that could distinctly identify human faces. These features (Eigen pictures) would then be represented linearly to recreate the face images in the initial training set. Assuming that the initial set consists of N images, PCA could form a set of K images, where $K < N$. Recreation anomalies could be reduced if the number of eigen pictures were increased putting in mind that their numbers would always be less than K. PCA is a standard linear algebra technique that is used in the automation of facial recognition technique.

At that time (1988), PCA was believed to be a break through because it demonstrated that less than a hundred Eigen pictures from a single face image would accurately be used to code a well reconstructed face image. In 1991 M. Turk and A. Pentland stretched their research and

discovered that the residual error from eigenfaces algorithm could be used to identify faces of images from an original set of images. They demonstrated how to represent eigenpictures as eigenvectors of covariance matrix that enabled computers perform Eigen - decomposition on a set of face images.

Unfortunately, the approach was limited by environmental factors such as lighting and complexity of the background, but it did not diminish the interest in furthering the development of automated face recognition technologies. In 2001, the technique drew a historic public attention with the help of the media in Super Bowl. Some of the areas were in field of security, psychology, and image processing, to computer vision. It could capture surveillance images from CCTVs and compare them to a large database of digitalized face images (eigenvectors). This revelation initiated the much-needed research and analysis on how the technology could be used to survey public needs while maintaining a considerable amount of privacy and social secrecy. Recently, the technique has advanced with the immergence of commercial applications such as TrueFace (1999) and FaceIt (1999).

Over the last fifteen years or so, automation of facial recognition has been an area of research focusing on pattern matching and pattern recognition, image analysis and identification of humans by their characteristics or traits (biometric authentication), (Zou et al., 2006). Facial recognition has also become an area of interest to security personnel and companies. It has been introduced as one of the various methods of identification and verification and was introduced in e-passports in 2004, (ISO, 2004; ANSI, 2004). Today, facial recognition technique is being used to mitigate passport fraud, identify lost children, and reduce benefit fraud.

2.3 Models for Face Recognition

Research in face recognition has intensified over the last 10 years due to the need for increased security and software applications that can help enforce the law. There are two basic categories of methods used in face recognition:

1. Appearance-based method,
2. Feature-based method.

Appearance-based method has achieved an enormous success in identification of human faces and as a result, has become the most popular method of face recognition. It uses the holistic facial appearance of a 2 dimensional image. Face images are captured using high resolution

cameras with high dimensionality, rendering an image of 1024 pixels and above. Performing facial recognition using original face images can be difficult without affecting their dimensionality. This will in turn reduce the accuracy with which the features can be extracted. Kirby and Sirovich, 1990 initially used PCA to extract features from a face image and used them to reconstruct human face image. This method uses a set of vectors that projects the face image data into a face space based on the variations in energy.

Turk & Pentland, 1991 introduced the eigenface method that incorporated PCA. Belhumeur, 1997 brought about the Fisherface method that incorporated linear discriminant analysis (LDA) to extract the most discriminant features and to reduce the dimensionality. LDA methods perform better than PCA methods as LDA uses the low-dimensional representation of face images, focusing mainly on the most distinguishable features in the image for extraction. LDA seeks for a set of projection vectors which form the maximum between-class scatter and minimum within-class scatter matrix simultaneously (Chen et al, 2000).

Other recent methods of image analysis that are gaining popularity in facial recognition include the frequency domain analysis methods e.g. the DFT (discrete Fourier transform), DWT (discrete wavelet transform) and DCT (discrete cosine transform).

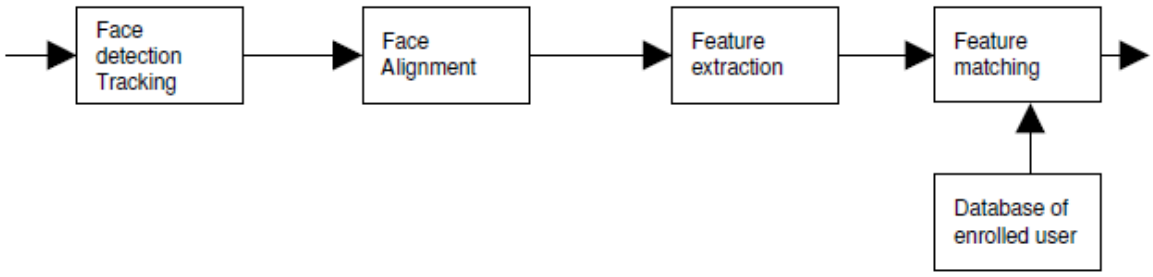


Figure 2.1: The process of facial recognition.

Face recognition classifies input image data into classes. The input data can be noisy due to environmental lighting conditions, complexity of the background scene, and pose among other factors. Every input signal has a pattern with which it occurs which is not absolutely random. These signals signifies the presence of some components e.g. the eyes, ears, mouth and nose in a face image as well as the relative distances between these components.

Figure 2.2: Examples of facial feature training templates

Figure 2.3: Synthesized images under variable pose and lighting.

2.4 Principal Component Analysis

In Principal Component Analysis, these objects are referred as eigenfaces or principal components. They can be extracted from the original signal (image data) by means of PCA, a mathematical procedure that uses orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of linearly uncorrelated variables, (Kyungnam Kim, 1990)

PCA transforms every input image of the training set into the corresponding eigenface. It enables the recreation of the original face image from the training data set by combining the eigenfaces, a most important feature of principal component analysis.

As a result, the initial face image can be achieved by reconstructing it from the eigenfaces if they are all added up in their right proportions.

Eigenfaces are distinct in that they represent unique characteristics of the original image and that is why their summation produces entirely, the original face image from which they were extracted. Therefore, for one to recreate the initial face image from the eigenfaces, a weighted sum has to be built from all the eigenfaces i.e. the reconstructed original image is equal to a sum of all eigenfaces, with each eigenface having a certain weight. (Matthew et al, 1991). These weights denote the degree to which the characteristic eigenface is present in the original image. An exact original face image can be reconstructed if all the features extracted from it are summed up exactly. But if a given proportion of the eigenfaces are used, the resulting image can only be an approximation of the original face image. Reconstruction of the exact original face image can only be achieved by minimizing the omission of some of the eigenfaces.

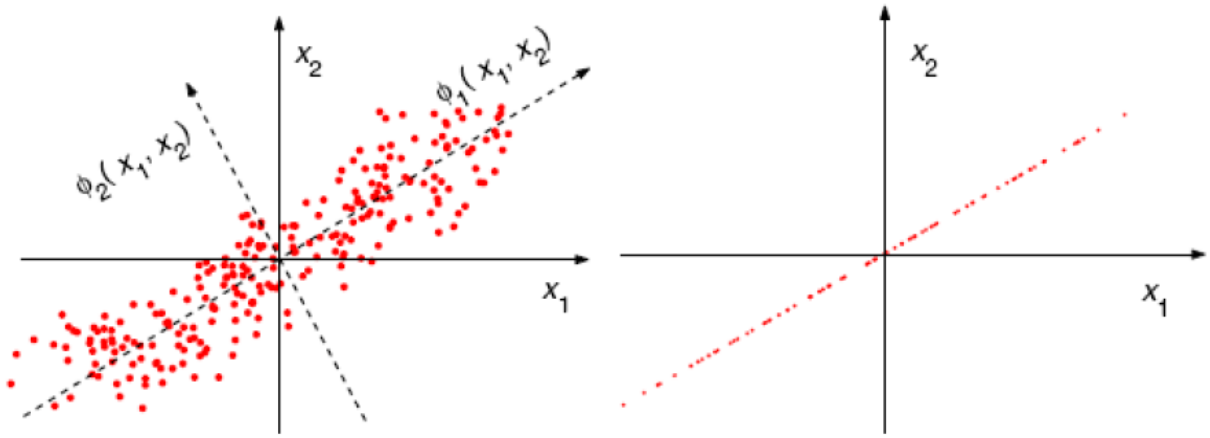


Figure 2.4: Principal Component Analysis Method

There are two things that can be determined from these weights:

1. Determine whether the image is a face or not, especially if the difference between the weighted sum of the image and that from the weights of face images is very large.
2. Determine the degree of similarity of different faces since similar faces may possess similar eigenfaces. If weights are extracted from all the face images available, they can be

grouped to clusters for easier reference. Similar faces are most likely going to have similar weights.

However, omission of some of the features may be unavoidable due to the limitations of the computational resources.

2.5 Facial recognition Evaluation Metrics

The performance of facial recognition algorithms is measured by:

1. False Rejection Rate (type 1 Error) and,
2. False Acceptance Rate (type 2 Error).

Type 1 and type 2 errors are inversely proportional to each other i.e. if a particular facial recognition system tightens its threshold value to disallow unauthorized individuals in an attempt to minimize FAR, it may end up improperly rejecting other authorized users.

Therefore, it is important for application system developers to provide a variable threshold value to strike a balance. A system aiming at rejecting unauthorized users by 100 per cent may cause a 4 per cent rejection rate to genuine and authentic users.

A system is considered having a good discriminating power if both false rejection and acceptance rates are relatively low (Shang-Hung Lin, 2000) i.e. reducing the area under FAR and FRR. This can be achieved by having good sensor devices, a good feature extraction scheme, and a powerful pattern matching and pattern recognition algorithm.

2.6 A Survey on Automated Teller Machine

This section discusses the security problems facing an ATM, its requirements, implementation issues and challenges after deployment.

2.6.1 ATM cards:

An ATM card is a PIN-based card; a plastic card used to withdraw money from a banking institution's automatic teller machine (ATM). Sometimes this card may also be used as a debit card, but not all ATM cards have this capability.

2.6.2 Safety Issues

Security is a significant aspect in any networked environment with the introduction of the state-of-the-art internetworking technology. This has enabled communication of machines across networks such that machines in different networks can communicate with each other by sending data across the network.

Danger lies with an exposure to all kinds and forms of threats and attacks in such an open environment. Some of these network technologies call for a redesign of their security mechanisms to provide non-intrusive security services to ATM machines.
They enable doorstep financial services telecommunication networks. They are connected by a grid of network of switches.

Some of the safety issues include:

1. If your ATM card is stolen the thieves can have an easy time of swiping the card to swipe your money.
2. Thieves don't even need the victim`s ATM card, as long as they have your name and card number. They can shop online or over the phone with your card information.
3. Can be hacked with sniffed usernames, passwords, PIN and bank accounts.
4. Every time you want to put a capital letter, full stop, comma etc. to strengthen your password, you find that it is not supported by some keypads, and the more restrictions you put on passwords, the harder they are to crack.
5. There is the worry about the variety of keypads variations in different countries.
6. Certain characters are treated differently by the different user registries.

2.6.3 General activities in a standard ATM

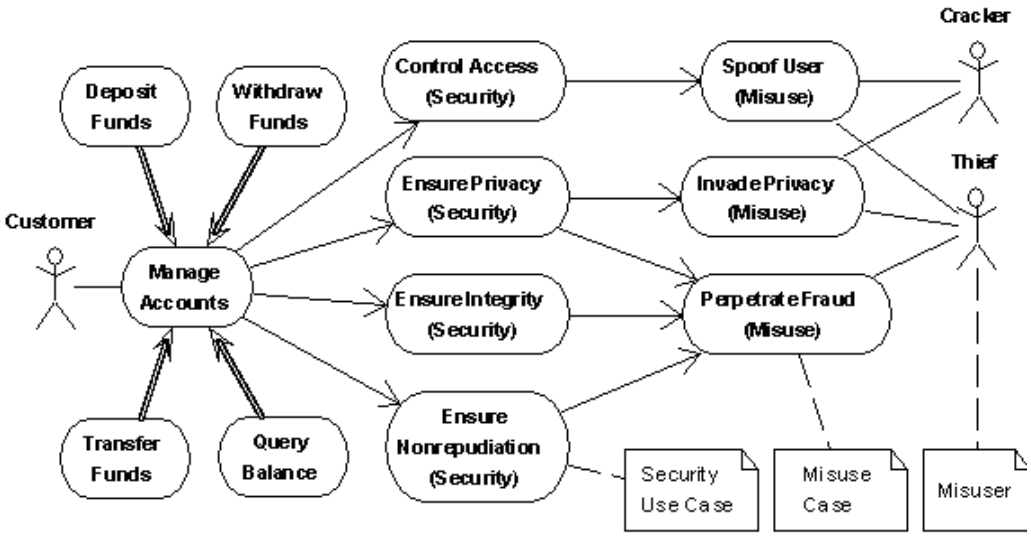


Figure 2.5: Activities in a standard ATM

2.6.4 Threats to ATM machines

ATM machines and networks suffer a lot of threats due to the fact that they are public utilities and that there are no measures to control who accesses them at any one point in time. Some of the threats include:

Eavesdropping: This is defined as a threat in which attacker accesses communication between ATMs by connecting into the transmission media and gaining unauthorized access to the data in transit. This threat has been categorized as a common occurrence to ATM networks.

Spoofing: This is where the attacker pretends to be someone else and attempts to access the victim`s information.

Denial of service: This occurs when ATM machines cannot perform their work and prevent their users from accessing their services.

Corruption of Information: This is the alteration of data in transit, deleting it, changing it and causing delay of its delivery to its recipients.

Forgery: Refers to when fake data is sent and is claimed to have been received.

Impact of ATM fraud on: share prices, relations with regulators, reputation brand, business relations and employee morale.

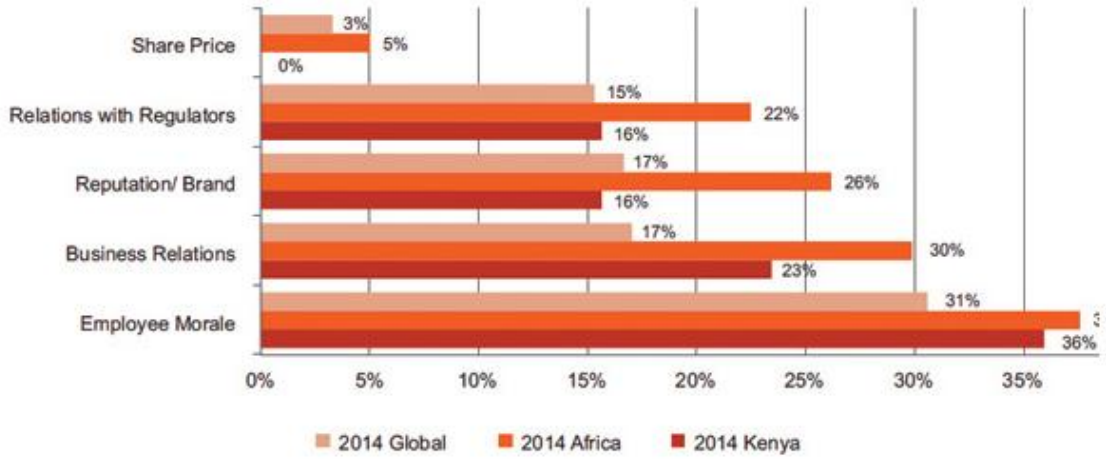


Figure 2.6: ATM Fraud in Kenya (Michira, 2014)

Cash skimming at ATMs has been on the rise, with the emergence of new tricks by hackers. The figure below shows the financial losses that were incurred in Europe through ATM attacks.

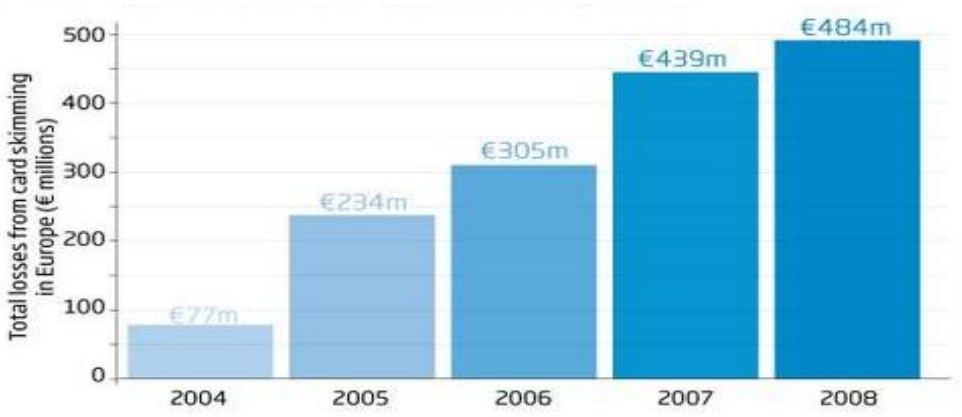


Figure 2.7: Cash fraud through ATMs in Europe (Chris Skinner, 2010)

2.6.5 Requirements of ATM security system

Access control is very important in ATM machines as it is in other financial-service renders. According to these objectives, the principal functions which an ATM security system should provide are as follows (Donglin Liang, 1997):

1. Verification of Identities: The Security system is expected to establish and verify the claimed identity of any user in an ATM.
2. Controlled Access and Authorization: Users should not be in a capacity to gain access to information or resources if they are not authorized to do so.
3. Protection of Confidentiality: Clients` data should be held with utmost confidentiality.
4. Protection of Data Integrity: The security system should guarantee the integrity of the data.
5. Strong Accountability: An entity cannot deny the responsibility of its performed actions as well as their effects.
6. Activities Logging: It should support the capability to retrieve information about security activities with the possibility of tracing this information to individuals or entities.
7. Alarm reporting: The security system should be able to generate alarm notification about certain adjustable and selective security related events.
8. Audit: When violations of security happen, the system should be able to analyze the logged data relevant to security.
9. Security Recovery: The security system should be able recover from successful or attempted breaches of security.

10. Security Management: The security system should be able to manage the security services derived from the above requirements.

2.7 An analysis of Models of face recognition

Handling intra-personal and inter-personal facial variations is a major challenge in face recognition systems. It is difficult how to appropriately measure the similarity between human faces under significantly different settings e.g. pose, illumination, and expression (Qi Yin, 2011). Several models have been developed in this regard and can be categorized into three forms:

1. Theoretical: Coarse-scale, ill defined, can be vague.
2. Information Processing: Specifies individual components and relationships between them.
3. Computational: Must be precise, specifies operations within individual boxes.

2.7.1 Hay and Young (1982) face recognition model

Hay and Young (1982) model outlined stages of face recognition as follows:

Face →Identity →Name

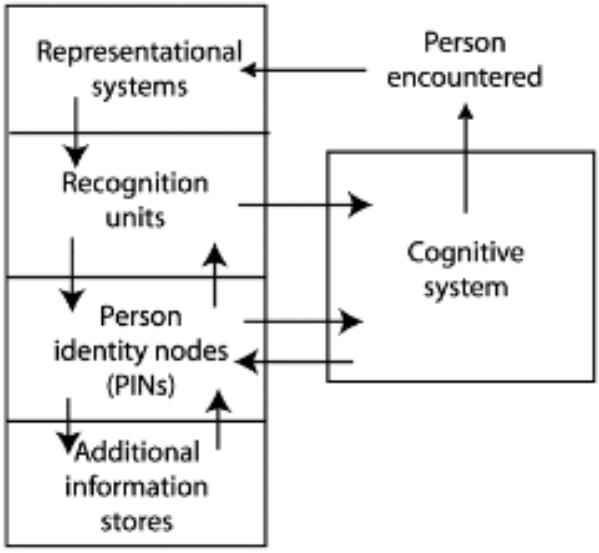


Figure 2.8: Hay and Young (1982) face recognition model

2.7.2 The Bruce and Young (1986) model

This model supports face recognition unit before PIN. A user is not granted access to the system unless the face is recognized, to proceed to the PIN phase after which the name of the user is generated and access granted. Faces recognized as familiar more quickly are classified by the occupation of the user.

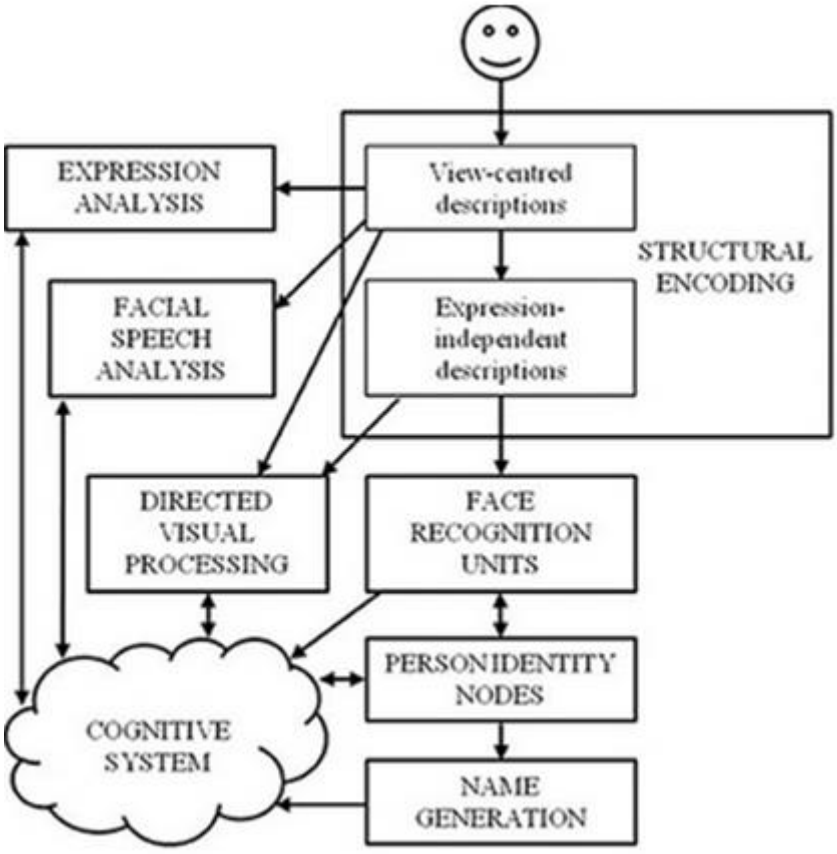


Figure 2.9: Bruce and Young (1986) model

The model has four main units:

FRU - face recognition unit

PIN - person identity node

SIU - semantic information unit

NIU - name input unit

FRU activates PIN unit→PIN activates Royalty SIU→Royalty SIU activates PIN→PIN now activated. The face recognition unit is activated by a match to a stored face representation in the database. The person identity node contains semantic information about the person.

Advantages

1. Configurational processing tolerates linear and global distortions of input.

Disadvantages

1. Any single manipulation (scrambling, inversion or blurring) leads to some but not total impairment.
2. Combinations of manipulations that affect different processes will severely impair recognition (scrambling + blurring or inversion + blurring = chance performance.).
3. Upright (but not inverted) faces are processed in an integrated holistic way, that prevents easy access to their constituent features
4. Features are recognised better if they are presented within a whole face than if presented in isolation or within a scrambled face (Tanaka and Farah 1993).
5. Blurring impairs processing of local features more than processing of global configuration (Costen et al. 1994)
6. Scrambling and inversion impair configural processing more than featural processing (Valentine, 1988)

2.7.3 The IAC model of face recognition (Burton et. al, 1990)

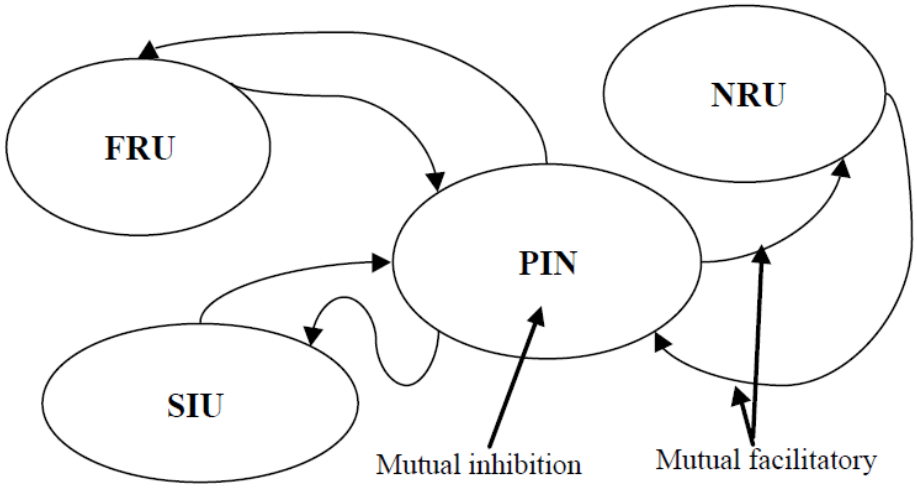


Figure 2.10: Bruce and Young (1986) model

How is this model different? FRUs signal face familiarity, PINs are modality-free gateways to semantic information. Details of connectivity and the spread of activity are clarified. No separate nodes for names, these are semantic information and are pooled accordingly. Names are poorly integrated with semantics.

Benefits of the Burton et al. model

1. The model successfully simulates a variety of phenomena i.e. relative timing of familiarity, semantic access and naming.
2. Familiarity faster-than Semantics and Semantics faster-than Naming

Disadvantages

1. It is unable to overtly recognize famous people. Could not identify a famous face in a pair (18/36), but could choose the famous name from a pair (29/32).
2. It slowed when asked the occupation of an individual when presented with a name + face from somebody with a different occupation.
3. Could only recognize two of the faces he had viewed, confirming that priming must have occurred sub-consciously (covertly)

Weakening the connections between FRU's and PINs enabled them to simulate all of the phenomena demonstrated by PH.ME could judge familiarity, but could not retrieve autobiographical information.

This suggests that SIUs and PINs were disconnected. However, Names and Faces could be paired; Hann et al. (1991) tested this prediction and found it to be correct (23/26).

In this model, activity doesn`t have to pass through SIUs to reach names.

2.7.4 Associate-Predict model (Qi Yin et al, 2011)

Associate-predict model is built on an extra generic identity data set, in which each identity contains multiple images with large intra-personal variation (Qi Yin et al, 2011). When two faces are considered under different settings such as non-frontal and frontal settings, one input of the face is associated with alike identities from the generic identity date set. Using the associated faces, the appearance of one input face is predicted under the setting of another input face, or

discriminatively predict the likelihood whether two input faces are from the same person or not. The two prediction methods above are called **appearance-prediction** and **likelihood-prediction**. By leveraging an extra data set i.e. memory and the associate-predict model, the intrapersonal variation can be effectively handled. To improve the generalization ability of our model, (Xiaoou Tang et al, 2011) further added a switching mechanism which they directly compared the appearances of two faces if they had close intrapersonal settings; otherwise, they used the associate-predict model for the recognition.

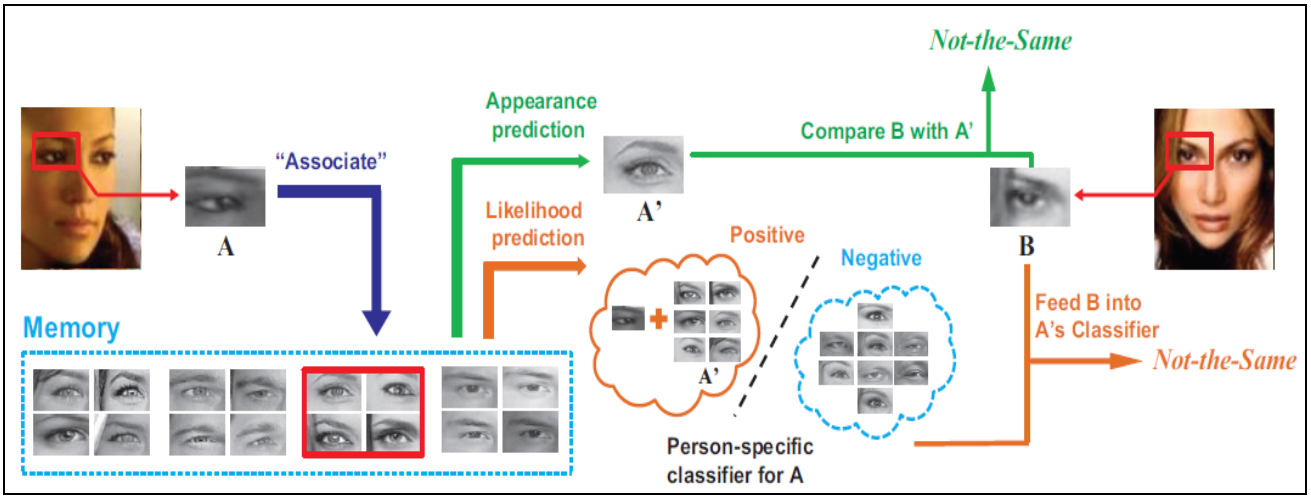


Figure 2.11: Associate-Predict model

A and B are two faces of the same person with significantly different settings i.e. pose, lighting, and expression. In their model, they associate a similar generic identity of the face B at the first step. Then, they predict the new appearance (B') of B under the similar setting of A. Using the predicted new face(s), they performed an activity they called prediction based matching.

Advantages

1. Their model explicitly handles the intrapersonal variation issue in a more principled way: using generic identities as a bridge;
2. Used the prior knowledge adaptively by a switch model.

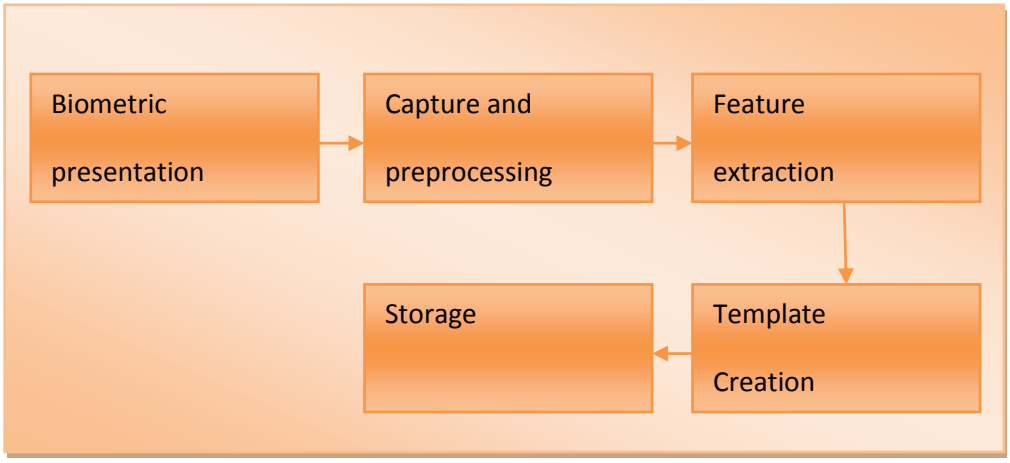
Disadvantages

1. It may reduce the inter-personal difference; it may be even worse than the direct appearance-based methods, especially when the input faces have very similar intra-personal settings.

2.8 How biometrics works

Biometric technology eases the manner in which users use a system. It eliminates the need to use or remember codes. It also gets lead of keyboards or keys for that meter. It boosts security and ease of use of a system, mainly emphasizing on presence.

A series of steps is followed to get the aimed goal as shown in the figure below:



1. Sensor: collects data (in this case a face image) and converts it into a digital format understood by the computer.
2. Signal processing algorithms: involves the quality control activities and development of the template
3. Data Storage: stores the processed data that new biometric templates will be compared to
4. Matching algorithm: it compares the probe image with other templates in store
5. Decision process: uses the results from the matching algorithm to make a decision.

2.8.1 Uses of Biometric Systems

1. National security- use of automated methods to determine an individual's identity

2. Law enforcement- used to secure countries from illegitimate trade and movement of people
3. Enterprise and E-government Services- administration of people, processes and technologies
4. Personal information and business transactions e.g. an ATM- business plans that meet customer demands for service at any time, from any location and through multiple communication device

2.9 Analysis of probable Biometric Modalities in an ATM machine

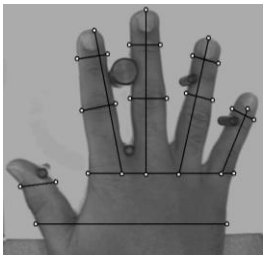
Fingerprint: Fingerprints have uneven surfaces of ridges and valleys that form a person's unique pattern, fingerprints are still widely used to date.

Face Recognition: The use of infrared detectors to capture a pattern of person's cranial physiognomy

Iris Recognition: Iris image processing is illuminating the iris with near infrared light, which takes the illuminated picture of the iris without hurting or causing any discomfort to the person.

Hand/ Finger Geometry: This is one of the first successful commercial biometric products. A person places their hand on a device and the system takes a picture of the hand using mirrors, the

picture shows top and side hand views, then measures digits of the hand and compares to those collected at enrollment.



2.9.1 Most suitable implementations

Out of all the biometrics modalities I have chosen Facial recognition as the best technique for my project. This is because of the many algorithms that can make it more secure and more easy to use.

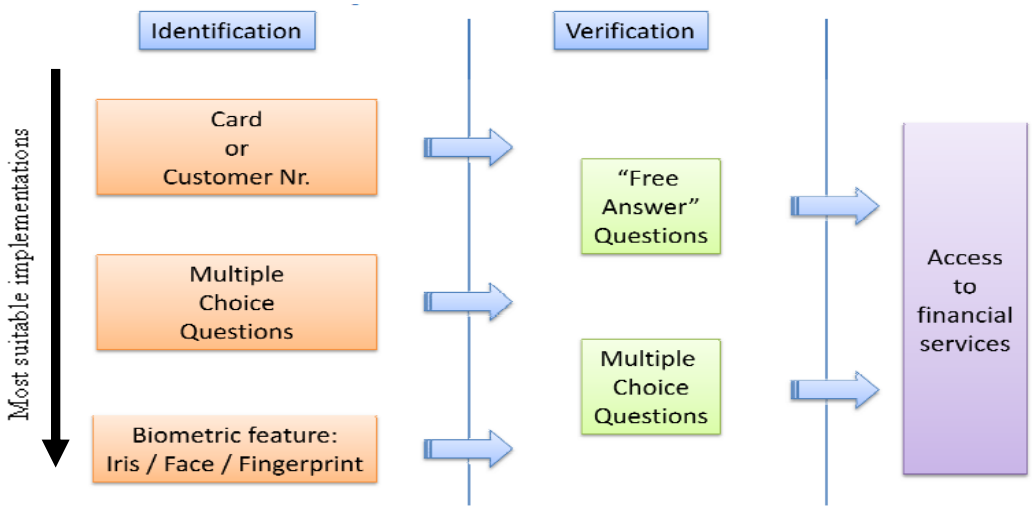


Figure 2.11: Most suitable implementations

2.10 Conceptual model

Definition: A conceptual model of an application is a representation of the application that the designer wants the users to understand and identify with (David W, 2011). An illustration of the application in a diagrammatic format, and the users reading the documentation, they build a conceptual model in their minds of how the application is used. It describes abstractly in terms of tasks, not keystrokes, mouse-actions, or screen graphics what users can do with the system and what concepts they need to be aware of (Austin, 2013).

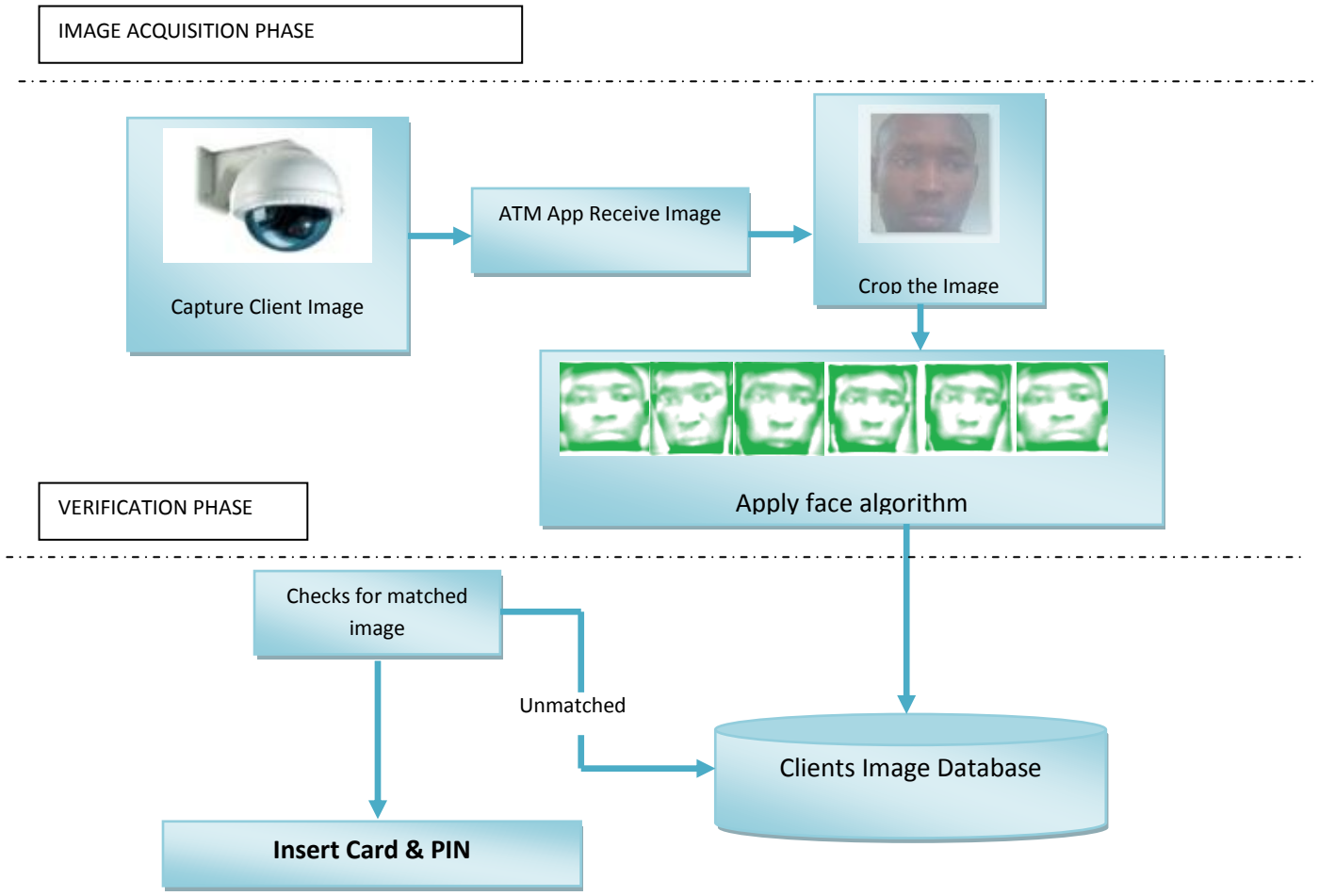


Figure 2.12: An illustration of the conceptual model

It allowed us to improve the recognition performance of our model by considering all the outputs. It calculates the Euclidean distance between the best/perfect and real output for

recognized person. When this distance is lower than the threshold we reject that person; otherwise the person is accepted.

2.10.1 Implementing security services on ATM

In this section, we discussed how to implement security services on ATM machine. We first examined the architecture of ATM and identified the ATM security scope, and then discussed how to place the facial recognition security feature in ATM architecture.

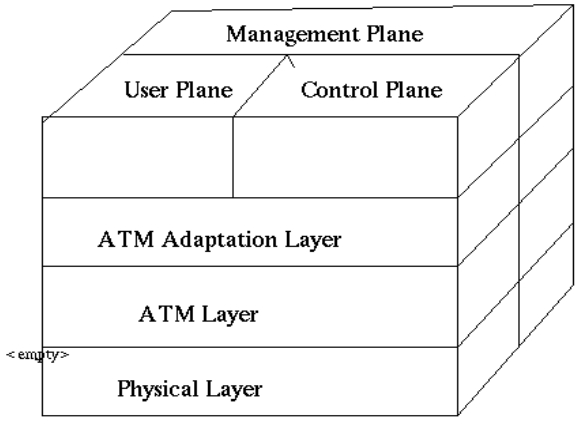


Figure 2.13: Standard ATM architecture

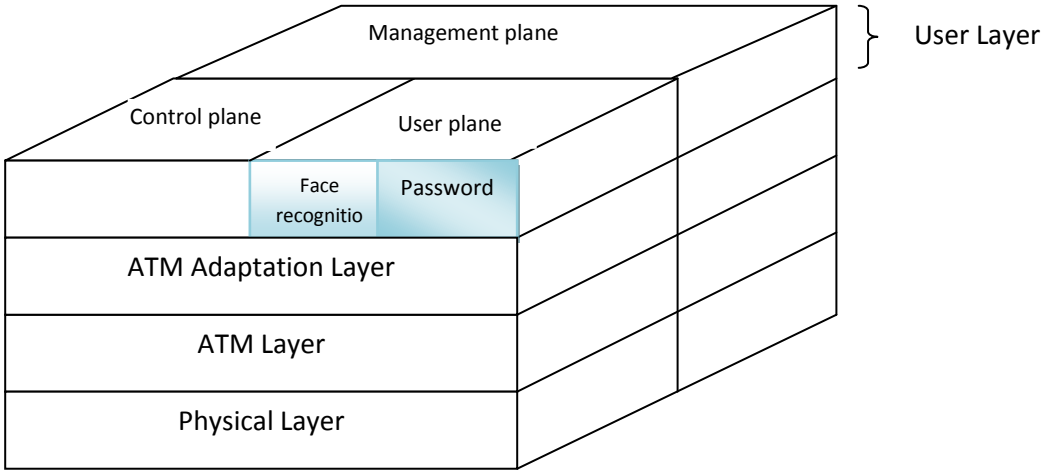


Figure 2.14: Extended ATM architecture

A standard ATM architecture includes three planes:

1. User plane
2. Control Plane

3. Management plane

A plane consists of entities that are responsible for transferring user data.

Entities in control plane deal with connection establishment, release and other connection functions. Management plane entities perform management and coordination functions related to both the user plane and the control plane, and functions related to establishment of a routing infrastructure. Besides ATM layer entities perform ATM data transfer on behalf of the other entities in the three planes.

2.10.2 The User Plane

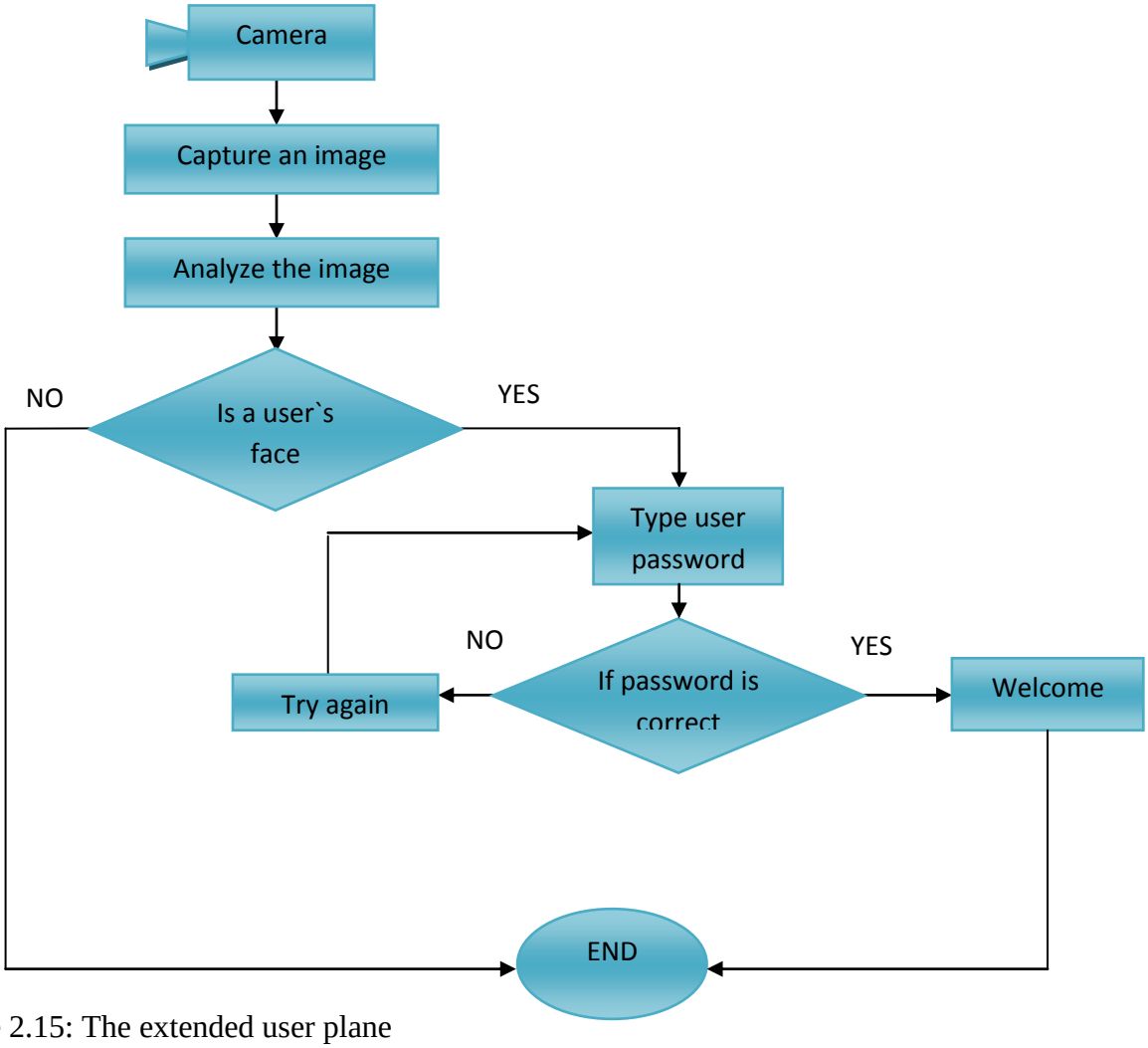


Figure 2.15: The extended user plane

According to figure 2.13, the user plane is the plane that directly interacts with user. Therefore, to meet the user's security objectives, user plane has to provide security services like access control, authentication, data confidentiality and integrity. Other services like key exchange,

certification infrastructure and negotiation of security options might be useful to meet the variety of the customers' requirements. Therefore they also should be supported by user plane. Providing different security services options is important because of the various traffic classes in ATM network. Different connections have different security requirements. User plane security services have to provide enough flexibility to meet these requirements.

2.10.3 Face recognition using Neural Networks

A neural Network is a computing system made up of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external inputs (Maureen Caudill, 1989). It is composed of a large number of highly interconnected processing elements (neurons) working in unison to solve specific problems. ANNs, like people, learn by example. An ANN is configured for a specific application, such as pattern recognition or data classification, through a learning process.

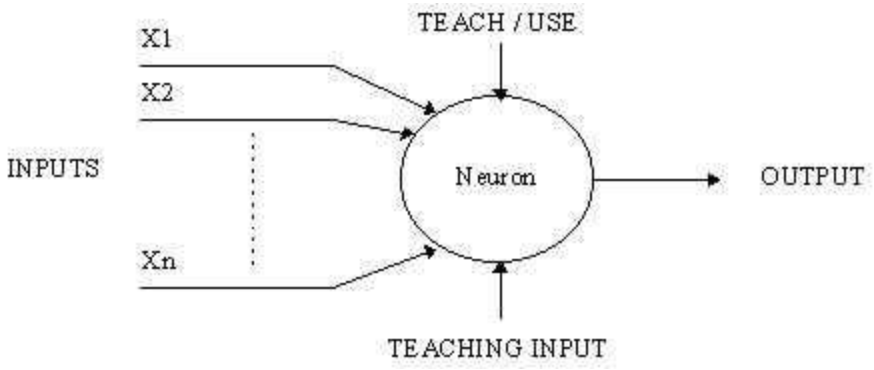


Figure 2.16: Artificial neural network

Neural networks are typically organized in layers. Layers are made up of a number of interconnected nodes which contain an activation function. Patterns are presented to the network via the input layer, which communicates to one or more hidden layers where the actual processing is done via a system of weighted connections (Christos, 2011). The hidden layers then link to an output layer where the answer is output.

A typical neural network

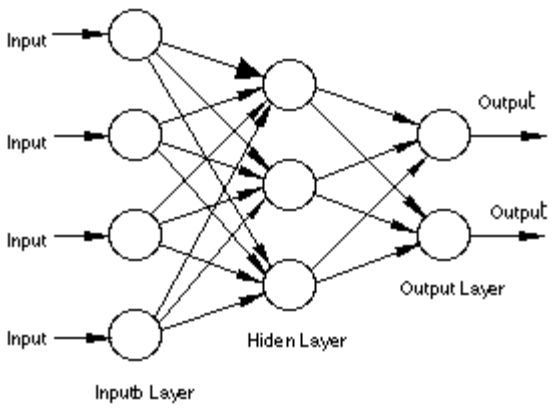


Figure 2.17: The three layers defining a neural network

Input for hidden layer is given by

$$net_m = \sum_{z=1}^{n} x_z w_{mz}$$

The units of output vector of hidden layer after passing through the activation function are given by

$$h_m = \frac{1}{1+\exp(-net_m)}$$

In same manner, input for output layer is given by

$$net_k = \sum_{z=1}^{m} h_z w_{kz}$$

And the units of output vector of output layer are given by

$$o_k = \frac{1}{1+\exp(-net_k)}$$

A neural network learning algorithm called back propagation is among the most effective approaches to machine learning when the data includes complex sensory input such as images (McGraw Hill, 1997). Face has about 80 characteristic parameters some of them are: width of nose, space between eyes, high of eyehole, shape of the zygotic bone and jaw width.

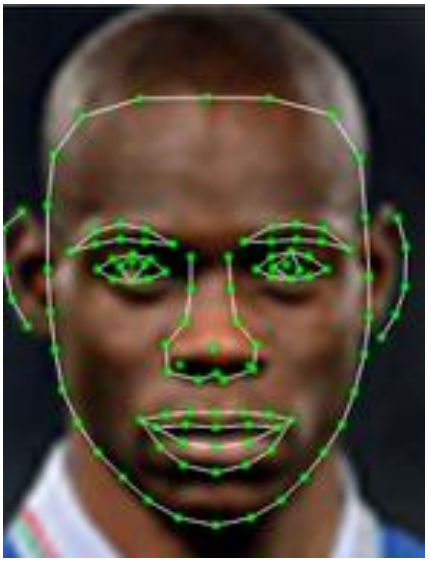


Figure 2.18: Face recognition using Neural Networks

Some distinct characteristics of the face used by artificial neural networks include but not limited to: distance between middles of the eyes, distance between middle of the left eyes and middle point of mouth, distance between middle of the right eyes and middle point of mouth, distance between middle of the left eyes and middle point of nose, distance between middle of the right eyes and middle point of nose, distance between middle point of mouth and middle point of nose, distance of middle point of the right eye and middle of nose, width of nose among others.

2.10.4 Placement of ATM Facial recognition Security component

After identification of the requirements and scope of ATM security, we discussed how to integrate our facial recognition component in the ATM network architecture.

According to figure 16 above, user plane is the plane that directly interacts with user. Therefore to meet the user's security objectives, user plane has to provide security services like access control, authentication, data confidentiality and integrity.

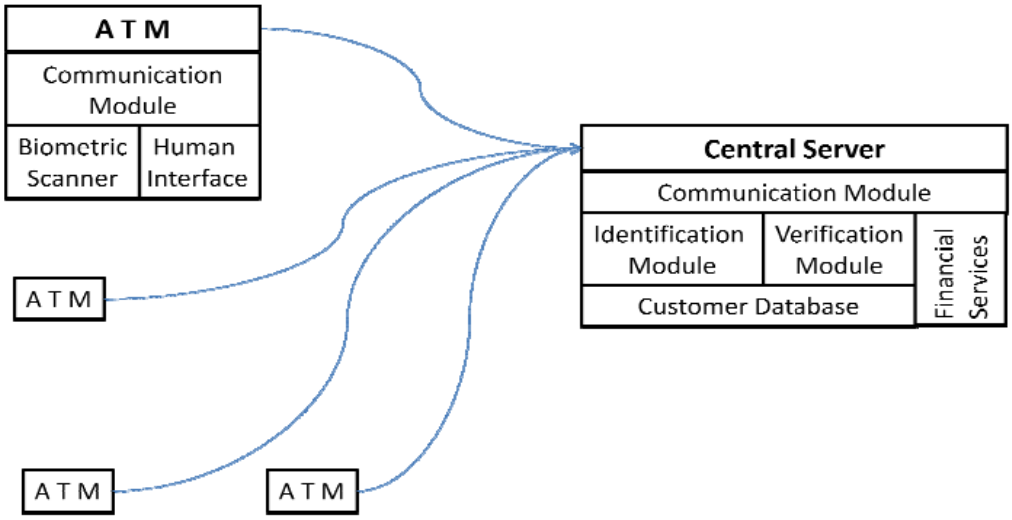


Figure 2.19: Expected effect, Client – Server Architecture

Presence detection: Upon entering the ATM terminal area, the camera detects the face of the person and captures it. It then attempts to match the probe image with stored images, upon which a successful match grants the user the rights to insert the card and proceed to financial services.

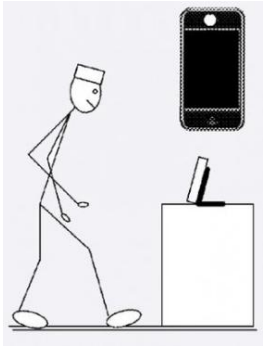


Figure 2.20: Presence detection

3.0 METHODOLOGY

3.1 Research design

Definition: it is an outline of how a research study will take place. The function of a research design is to ensure that the evidence obtained enables us to answer the initial question as unambiguously as possible (The Context of Design, 2014). It "deals with a logical problem and not a logistical problem" (Yin, 1989) it includes:

1. how data is to be gathered,
2. what equipments will be used,
3. how the equipments will be used and
4. The intended means for analyzing data collected.

3.1.1 Design type

Experimental design: An Experimental Design is the laying out of a detailed experimental plan in advance of doing the experiment (NIST, 2012).

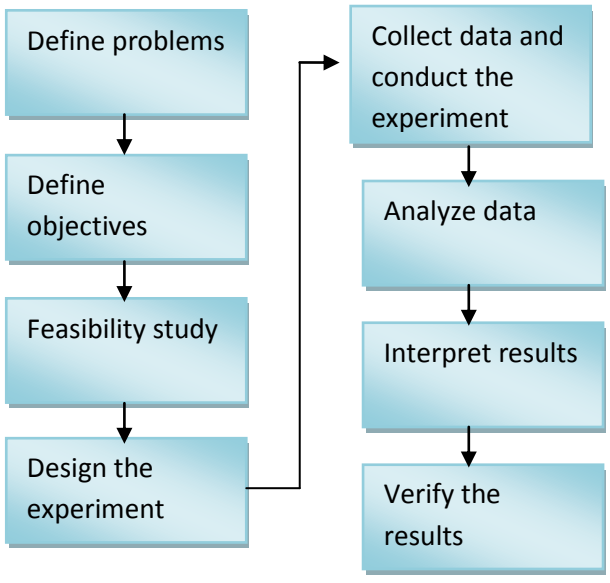


Figure 3.1: Experimental design

3.1.2 Objective

Identify the faults of the currently used PIN for authentication in ATMs and making suggestions for adopting face recognition and how it can be improved.

3.1.3 Process variables

Input variables

Input variables are the facial images and the personal details of the users, for the purpose of identification.

Output variables

A database of personal details and face images against which given images will be matched

3.1.4 Constraints, guidelines and assumptions

Software constraints

1. Operating system: Windows 2000 and above.
2. Database: MySQL

Hardware constraints

Camera or webcam for image acquisition purposes.

Software guidelines

The code is kept tidy and straightforward to ease future program upgrades and maintenance.

Assumptions

Users will provide face images with acceptable quality.

3.2 Data

The research data that has been collected is for the purposes of analysis to generate original research results. It has been gathered, reviewed, and analyzed to help in forming finding and conclusion on face recognition. Quantitative data analysis was used to help draw the results.

3.2.1 Data collection method

The choice of method is influenced by the data collection strategy, the type of variable, the accuracy required, the collection point and the skill of the enumerator. In this case, questionnaire was used.

3.2.2 Data Sources

Our main source of data was from bank customers (clients who do cash deposit and withdrawal from ATM machines); consumers at the level where the products are finally consumed.

3.3 The internal functions

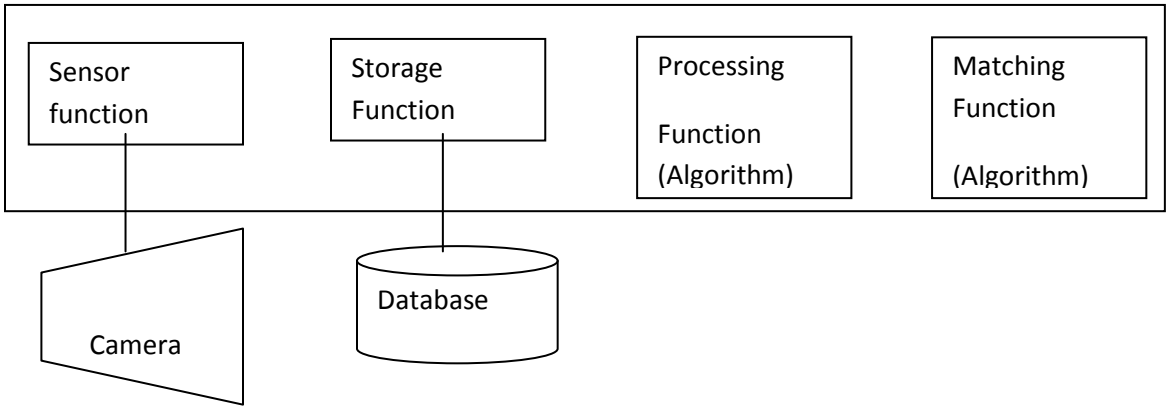


Figure 3.2: Internal functions of the system

3.4 Data flow diagram

This design shows the flow of data through the various system modules.

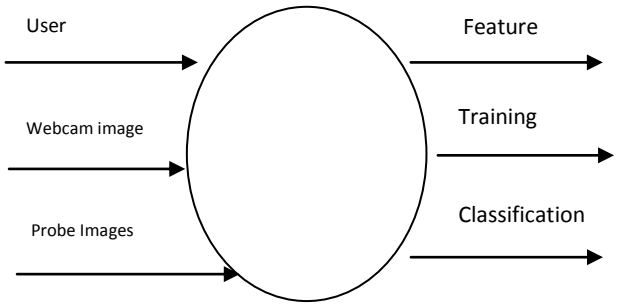


Figure 3.3: Data flow diagram

3.5 Object Relationships.

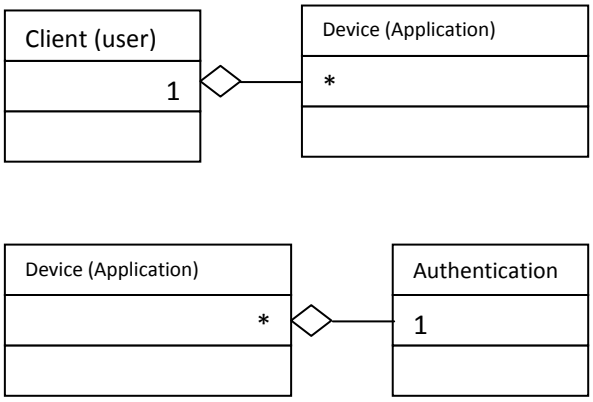


Figure 3.4: Object Relationships diagram

3.6 Use Case Diagram for the System

A use case is a set of scenarios that describe an interaction between the user and the system. The diagram displays the relationships among the actors and use cases. An actor represents a user or another system that will interact with the system to be modeled. The use case is an external view of the system that represents some action that the user might perform in order to complete a task.

The tasks performed by the student and the Administrator are as follows

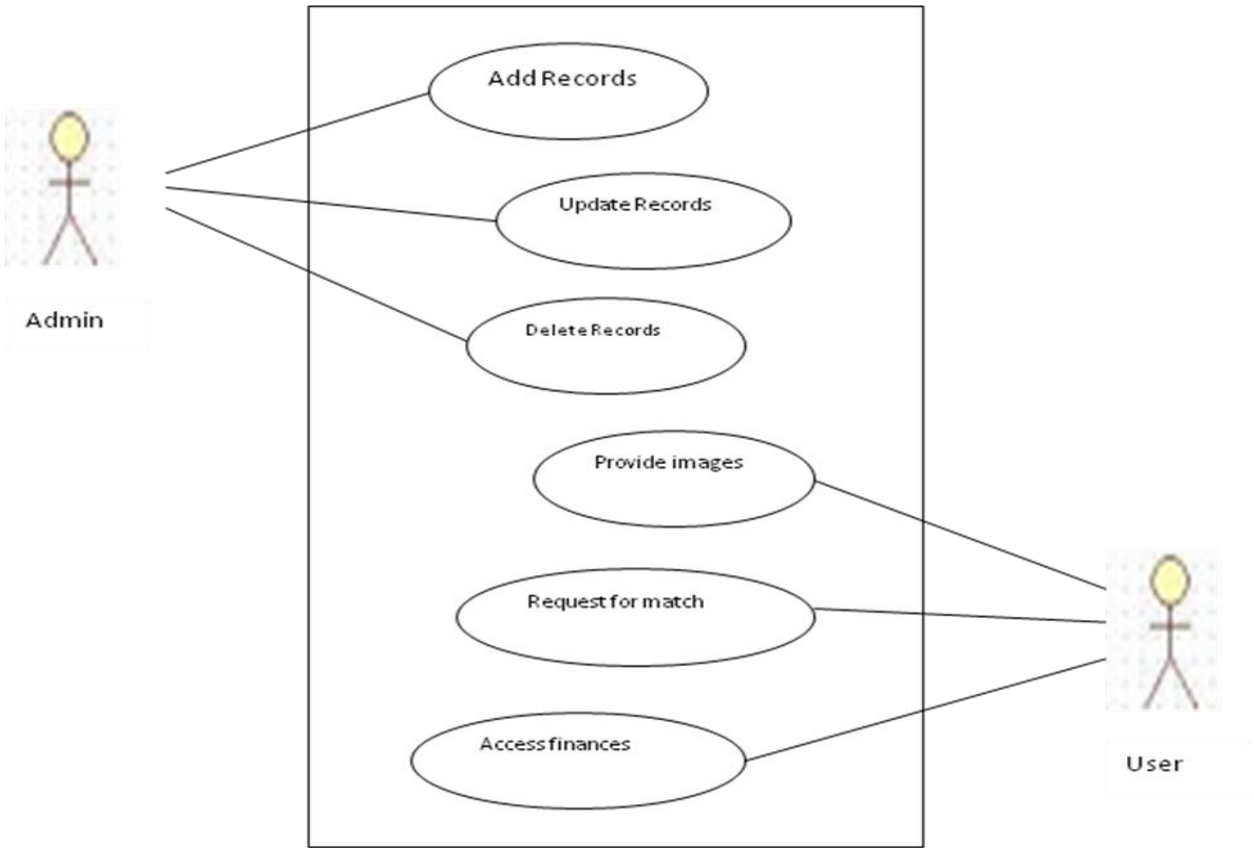


Figure 3.5: Use case diagram

3.7 Class diagrams

These are used to describe the types of objects in a system and their relationships. They model class structure and contents using design elements such as classes, objects and packages. A class represents an entity of a given system that provides an encapsulated implementation of

certain functionality of a given entity. The properties of a class are called attributes. A class represents by a rectangle by a rectangle.

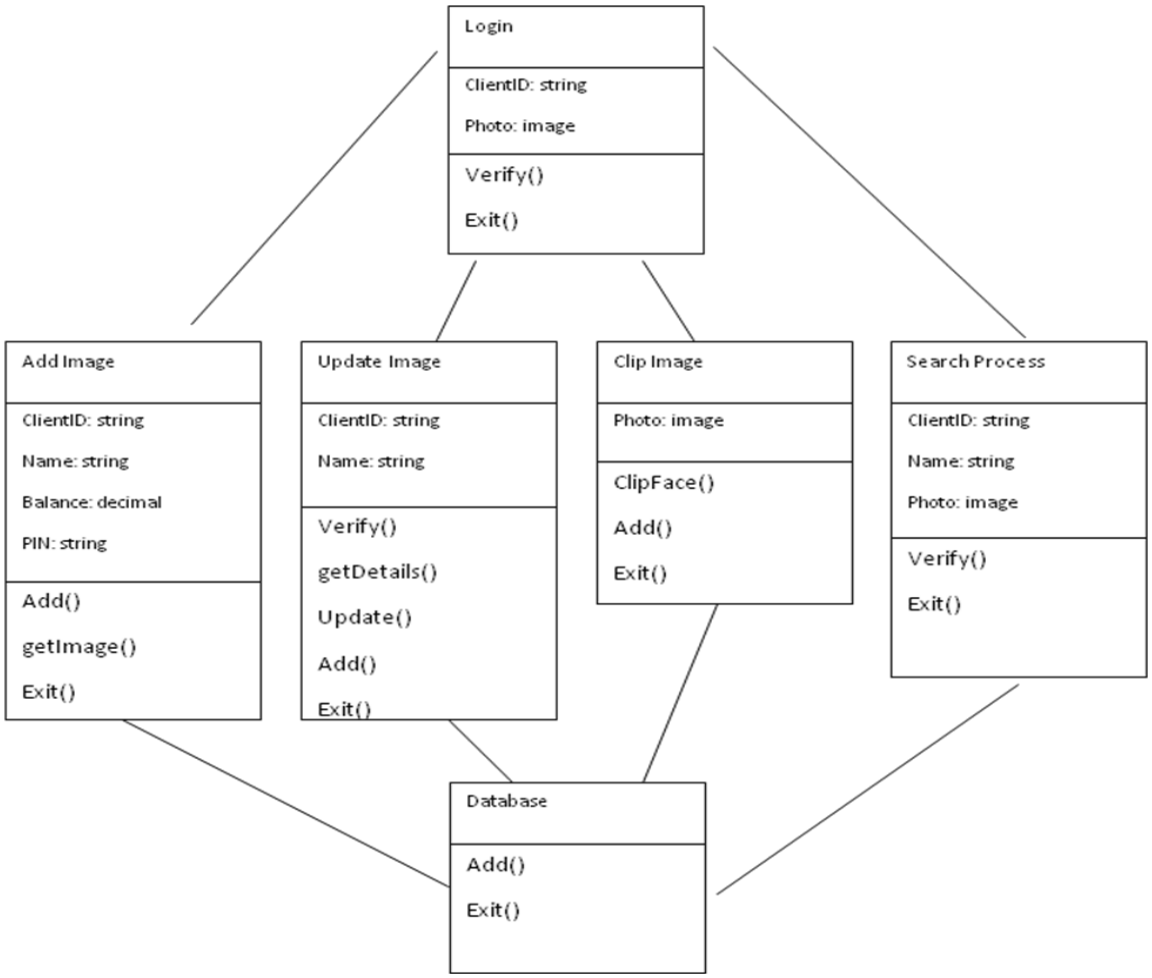


Figure 3.6: Class diagram

3.8 Sequence Diagram

UML Sequence diagrams are an easy and intuitive way of describing the behavior of a system by viewing environment. A sequence diagram shows an interaction arranged in time sequence.

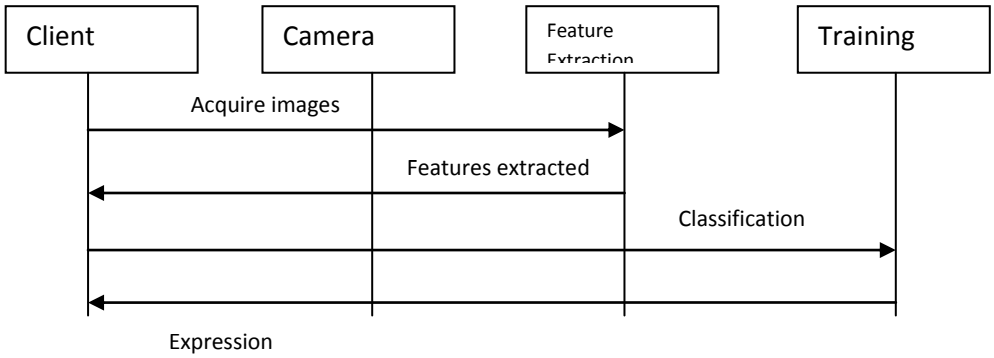


Figure 3.7: Sequence diagram

3.9 State diagram

State diagrams are used to describe the behavior of a system. They describe all the possible states of an object as an event occurs. They demonstrate the behavior of an object through many use cases of the system.

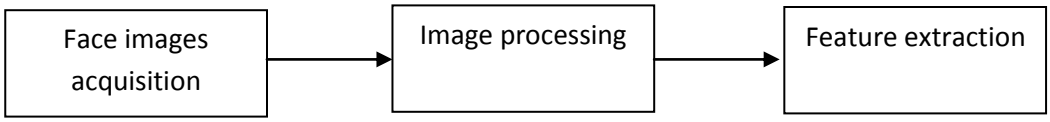


Figure 3.8: Sequence diagram

3.10 E-R Diagram

It shows the data entities, their associated attributes and the relations between the entities. It is widely used in database design.

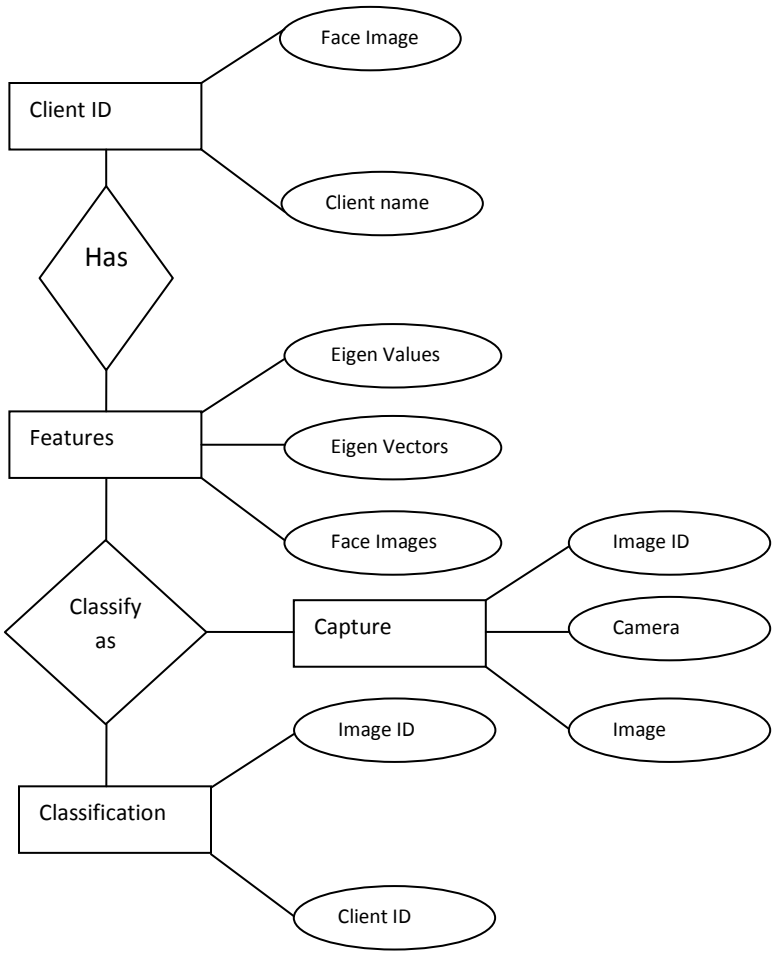


Figure 3.9: Entity relationship diagram

3.11 Database Design

Table 3.1: Users details

Fields	Type	Size	Description
UniqueID	Int		Enter unique id
User Name	Varchar	50	Enter the name
PIN Number	Varchar	20	Enter mobile number
Balance	Varchar	50	Enter email address

Table 3.2: Images table

Fields	Type	Size	Description
UniqueID	Int		Enter the serial number
Image1	Varbinary	MAX	Enter the a images
Image2	Varbinary	MAX	Enter the b images
Image3	Varbinary	MAX	Enter the c images
Image4	Varbinary	MAX	Enter the d images
Image5	Varbinary	MAX	Enter the e images
Image6	Varbinary	MAX	Enter the f images
Image7	Varbinary	MAX	Enter the g images
Image8	Varbinary	MAX	Enter the h images
Image9	Varbinary	MAX	Enter the i images

3.12 Prototype development

The designing and development of the prototype was used as a proof of concept. It was meant to display the functionality of two-factor authentication under development with the attempt of providing the exact logic of the original software.

3.12.1 Functional requirements

1. System must be able to identify human faces,
2. Must be able to search for faces in images as an input and search for a matching face in folder and then show the results,
3. The results should be viewed by showing the name of the face match of the input to the most similar face in the folder.

3.12.2 Non Functional Requirements

1. The user should be able to click on the “Capture” button.
2. Critical errors and information should be displayed to the user.
3. The face should be localized by detecting inner and outer boundaries and the background should be ignored.
4. User should be able to save detected faces for future comparison.

3.12.3 Enrolment

In this phase, samples of face images are captured with a visual unit (camera) and processed in a form that can be held in a database. It involves:

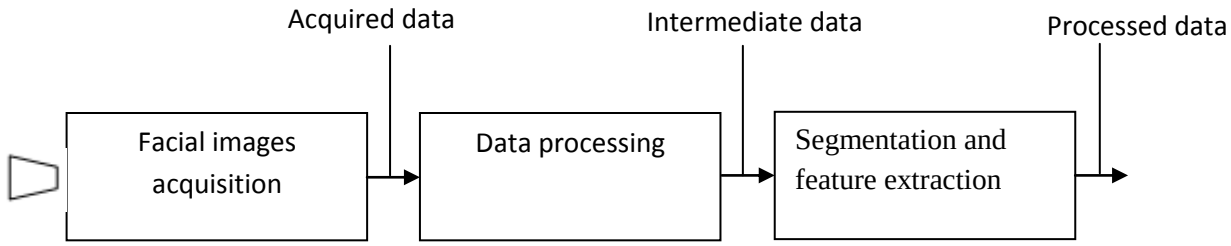


Figure 3.10: Functions of the biometric system

3.12.4 Performance Requirements

The system application should be used by only one face of the user. It can run on a duo core processor and above, using approximately 30% capacity of the processor.

It should not be below 256MB RAM while it is on action.

3.12.5 Development language

Java is the programming language that will be used in the development of the software together with the OpenCV libraries. The software architecture will be based on MVC (Model-View-Controller) architecture. It will run on Windows operating systems. Ms SQL Server will be the database server. It will store the datasets and related information of face features.

3.13 Design of the two-factor authentication model

This stage in the development involves translation of the system specifications in the analysis phase into a technical specification for implementation. The primary purpose of this system design phase is to specify various components of the system and their relationships and interaction in a format that can easily be mapped into programming codes to produce the required software.

The aim is to design a functional, an efficient, effective and easy-to-use system for use in the banking industry.

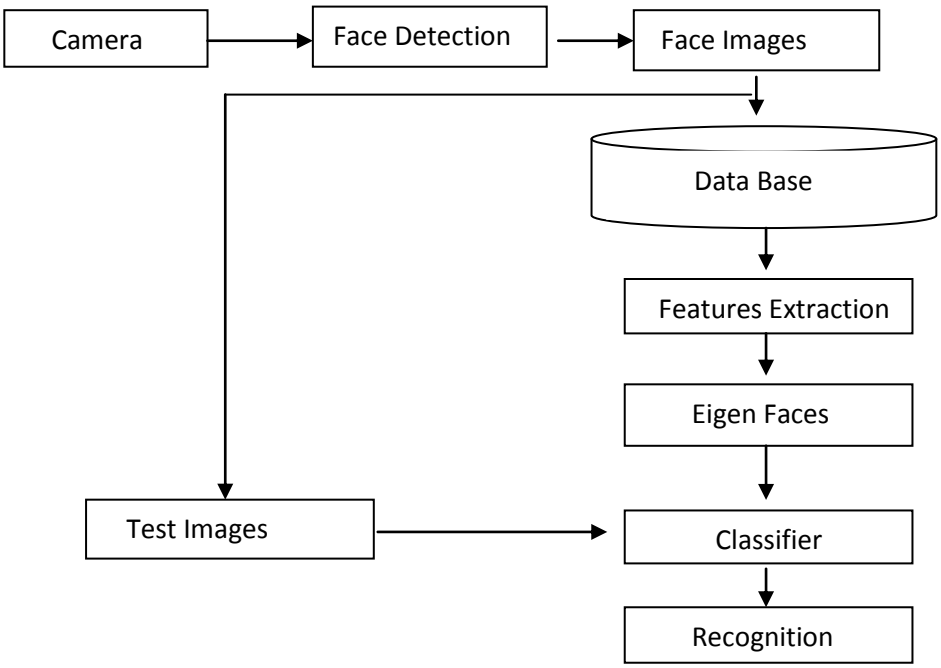


Figure 3.11: Design of Face Recognition

3.13.1 Rapid Application Development (RAD)

Rapid Application Development (RAD) is a development lifecycle designed to give much faster development and higher-quality results than those achieved with the traditional lifecycle (James Martin). It is designed to take advantage of powerful development software like CASE tools, prototyping tools and code generators (Rapid application development (RAD). 2011). It is a user-centered and incremental development approach. It is characterized by active user involvement, collaboration and co-operation between all stakeholders. Testing is integrated throughout the development life cycle so that the system is tested and reviewed by both developers and users incrementally. The key objectives of RAD are:

1. High Speed
2. High Quality
3. Low Cost

3.13.2 Components of Rapid Application Development:

Requirements Planning

Also referred to as the Concept Definition Stage; Requirements planning defines the business functions and data subject areas that the system will support and determines the system's scope.

User Design

Also known as the Functional Design Stage, this stage uses workshops to model the system's data and processes and to build a working prototype of critical system components.

Rapid Construction

Also known as the Development Stage, this stage completes the construction of the physical application system, builds the conversion system, and develops user aids and implementation work plans.

Implementation

Also known as the Deployment Stage, this stage includes final user testing and training, data conversion, and the implementation of the application system.

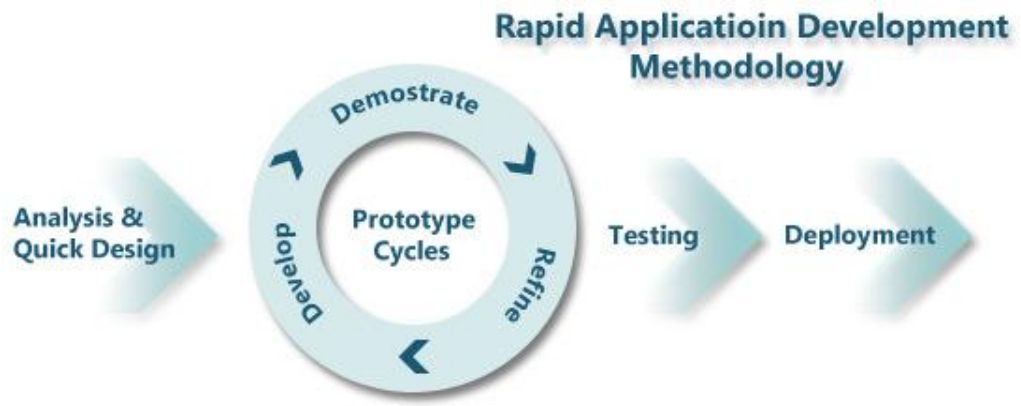


Figure 3.12: Shows the necessary steps in Rapid Application Development.

Strengths of RAD

1. Takes advantage of automated tools and techniques to restructure the process of building information systems.
2. Replaces hand-design and coding processes, which are dependent upon the skills of isolated individuals, with automated design and coding, which is an inherently more stable process.

3. Give an Information Systems organization its first real basis for continuous improvement.
4. It is a more capable process, as it is much faster and less error prone than hand coding.

Essentials of RAD

Methodology involves selection of CASE tools for supporting the processes of modeling, prototyping and code reusability as well as automating many of the combinations of techniques.
People involve involvement of people with the right skills and talents for fast application development.
Management involves motivating both users and the IT staff, selecting and managing SWAT teams, and demonstrating through the use of performance measurements that RAD does mean speed, quality, and productivity.
Tools involve the use of both computerized tools and human techniques to achieve the goals of high-speed and high quality.

3.14 Tools required

Below is a list of items that will be required to accomplish the goals and objectives of this project:

1. Windows Operating System (at least Windows Professional)
2. Java Development Kit 17 or later
3. JAVA platform - Net Beans
4. VeriLook SDK
5. Java Media Framework
6. Relational Database Management Systems

3.15 Justification of the methodology

The major strength of this methodology is its ability to track changes throughout the entire process. Each and every entity created in the analysis and design phases can be traced back or forth to related entities within the development framework.
Also it supports the development from requirements analysis to implementation.

4.0 IMPLEMENTATION, RESULTS & DISCUSSION

4.1 Methods and results

Our research covered four areas. In our first experiment, we explored the role of edges of a face in face recognition. We demonstrated that the performance of face recognition is drastically affected if only the edges of a face are presented for processing. In our second experiment, we looked at holistic and independent processing of facial features. Our third experiment explored the relationship between the width and height dimensions of a face image while our fourth experiment focused on effects of vertical inversion of images on both human vision and computer recognition. The specific experiments and results for each study have been described below.

4.1.1 Experiment 1: Examining the role of edges of a face in face recognition

Experiment 1 examines the role of edges and the outline of a human face in face recognition. We found out that edge-maps are a powerful initial representation for visual inputs. According to Richard Russell et al, 2005, they "capture the most important aspects of images, while being largely invariant to shallow shading gradients that are often the result of illumination variations". Line-drawings are sufficiently recognized by human vision with quick pen portraits being often highly recognizable. Such images have a relatively high spatial frequency enough for facial recognition. They possess considerable contour information for defining luminance relations. Bruce et al, 1998 argued that these depictions possess photometric cues and contours that embody face's photometric structure. Pearson and Robinson, 1985 convincingly argued that such inclusions make human-generated line drawings better recognizable than computer-generated images.

Figure 4.1: Face images containing contour information may be difficult to recognize.

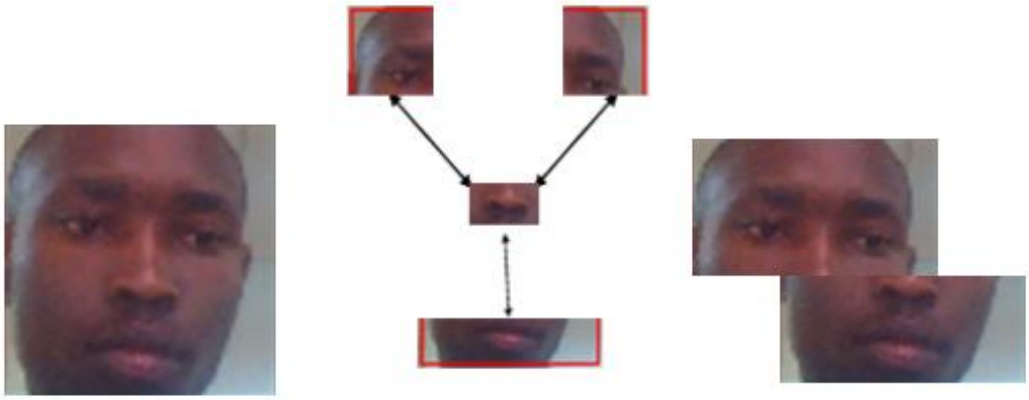
4.1.2 Experiment 2: Holistic vs. Independent processing

Experiment 2 tests whether facial features are processed holistically or independently from the rest of the face. Human vision can often identify a face from very little information such as eyes, nose, mouth, chin, eyebrows, among others. Sadr et al, 2003 argues that a single feature such as the eyes or the eyebrows can be sufficient for recognition of various famous faces.

However, if the features present on the upper half of a face are combined with those on the lower half of a different face, it becomes difficult to do recognition on the two distinct identities.

Thus, the holistic approach seems to affect the manner in which distinct features are processed. If the two halves (top and bottom halves) of the face are misaligned thereby interrupting holistic processing, recognition of the two identities is easily carried out.

These experiment suggests that facial recognition is dependent on holistic processes involving an interdependency between featural and configural information (Pawan Sinha et al, 2005).



Holistic vs. Independent processing

Figure 4.2: Face recognition component found it difficult to perform Independent processing.

4.1.3 Experiment 3: Relationship between width and height of a face

Experiment 3 seeks to find the configural relationship between the width and height dimensions of a face image. We found out that human vision system does not entirely depend on such measurements. Human vision can recognize a face whose width and height dimensions have

been disrupted by a compression, extension or skewing of a face image up to a certain degree. From our experiment, we have established that there exists a notable tolerance of face recognition processes to extensive or compressive distortions. Faces can be compressed up to 25% of their initial height or width without losing all their recognizability. These compressions interfere with the distance between the face features (inter-feature distance) and the ratios of the x and y dimensions.

For human vision, disrupted dimensions and ratios do not interfere with recognition a great deal. They are able to encode such face images and this constitutes a useful strategy for computer vision as well. Drastic compressions or extensions of face images do not necessarily cause them unrecognizable. Faces can be compressed way down up to 25% of their original width while maintaining their recognizability and performance.

Figure 4.3: Effect on compression of faces

4.1.4 Experiment 4: Effects of vertical inversion of face images

Experiment 4 examines the effects of vertical inversion of images on both human vision and computer recognition. Our investigation shows that inverted face images are more difficult to recognize than upright images despite having the same information. Yin, 1970 displayed a series of face images to a set of individuals who had to identify them when upright and in an inverted form. Recognition performance in the experiment phase was 90 percent when the face images were in an upright form, but dropped down to a remarkable 62 percent when all the faces were inverted.

From Yin`s experiment, there was a drastic decline in performance up to 10 percentage when house images were used instead of faces.

We attributed the decline in face recognition performance stimulated by vertical inversion, to the fact that the transformation selectively disrupts computer vision ability to extract configural information from faces, while leaving featural processing largely intact (Pawan Sinha et al, 2005).

Other experiments on human face recognition performance have shown that face images differing in individual features i.e. eyes, nose and mouth can be easily differentiated even when inverted vertically but configurally harder to differentiate upon inversion.

We conclude that vertical inversion has a significant effect on computer vision performance and there should therefore be a clue on the face encoding strategy in various visual systems.

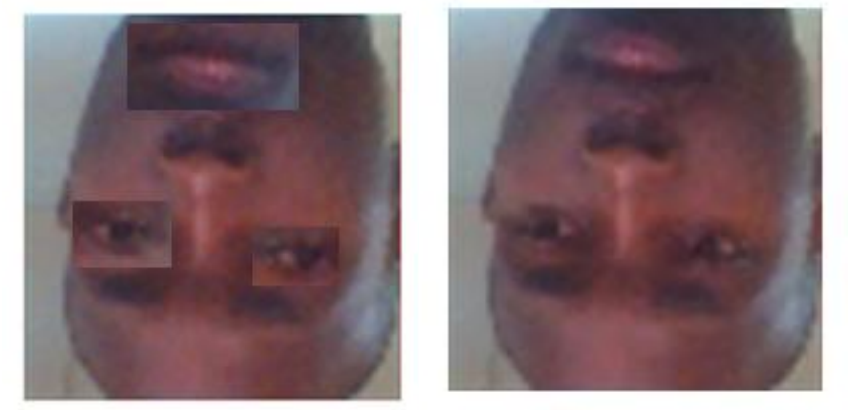


Figure 4.4: Thatcher Illusion

The eyes and mouth of the face image on the left are vertically inverted while the image on the right is wholly inverted.

Table 4.1: Authentication mechanisms chart

Authentication Mechanisms	Accuracy	Cost	Devices Required	Social Acceptability
Biometrics	High	Medium	Camera	High
PIN	Medium-low	Low	Keypad	High
Password	Medium-low	Low	Keypad	High
Pattern	Medium-low	Low	Scanner	Low
Smartcard	Medium	Medium	Card reader	High

Table 4.2: Biometrics comparison chart (Pbworks, 2006)

Biometric Technology	Accuracy	Cost	Devices Required	Social Acceptability
Face recognition	Medium	Medium	Camera	High
Fingerprint	High	Medium	Scanner	Medium
Iris recognition	High	High	Camera	Low
Retinal scan	High	High	Camera	Low
Voice recognition	Medium	Medium	Microphone	Medium

Table 4.3: Biometrics Comparison Chart (360biometrics, 2012).

Biometric Technology	Universality	Uniqueness	Permanence	Performance	Circumvention	Acceptability
Face recognition	H	M	M	M	L	H
Fingerprint	M	H	H	H	H	M
Iris recognition	H	H	H	H	L	L
Retinal scan	H	H	M	H	H	L
Voice recognition	M	L	L	L	L	M
H = High, M = Medium, L = Low						

Table 4.4: Biometrics Evaluations Chart (Debnath Bhattacharyya et al, 2009)

Biometrics	EER	FAR	FRR	Subjects	Comments
Face	NA	1%	10%	10	Varied light, indoor/outdoor
Finger	2%	2%	2%	25000	Rotation, skin distortion
Hand geometry	1%	2%	2%	129	Improper placement
Iris	.1%	4%	.99%	1224	Indoor environment
Keystroke	1.8%	7%	.1%	15	During 6 months period
Voice	6%	2%	10%	30	Textdependent

Facial scan is among other effective biometric indicators for human recognition. Different biometric technologies have been used in different identification application systems due to their variations in accuracy, ease of sensing, cost and intrusiveness.

Among the 6 biometric technologies considered in this research study, facial recognition got the highest compatibility as shown in the figure below (Fig. 4.1), in an Automated Teller machine based on a number of evaluation factors (R. Hietmeyer, 2000).

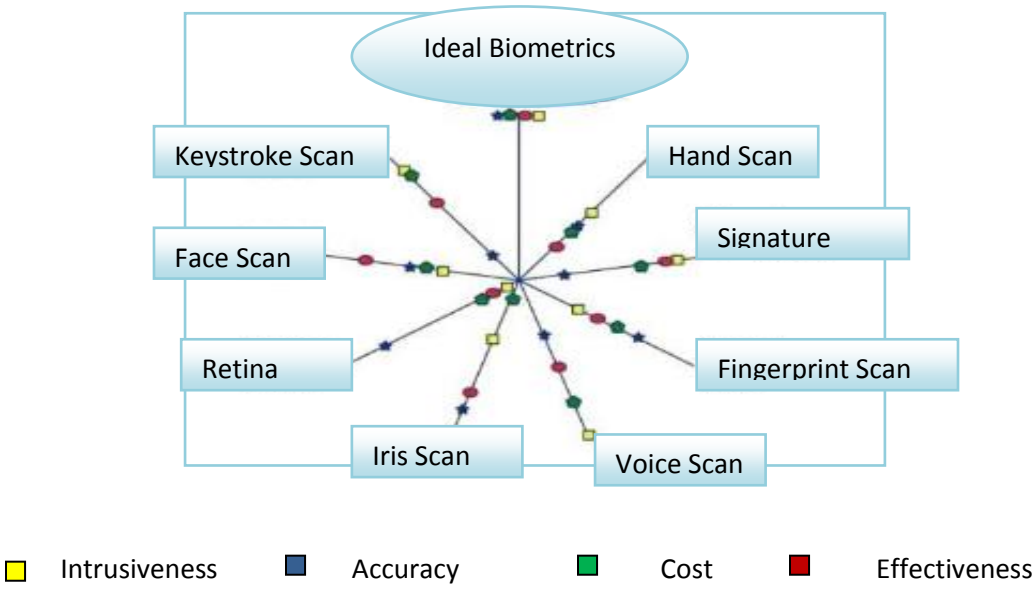


Figure 4.5: Comparison of various biometric features based on cost, effectiveness, intrusiveness and accuracy.

Each biometric indicator has its own unique proper ties, which means that each of them must be addressed independently when evaluating test results and selecting the most appropriate approach for a particular application. The most current evaluations of face recognition technology took place between September 1996 and March 1997 with the Feret (P.J. Phillips et al, 1998).

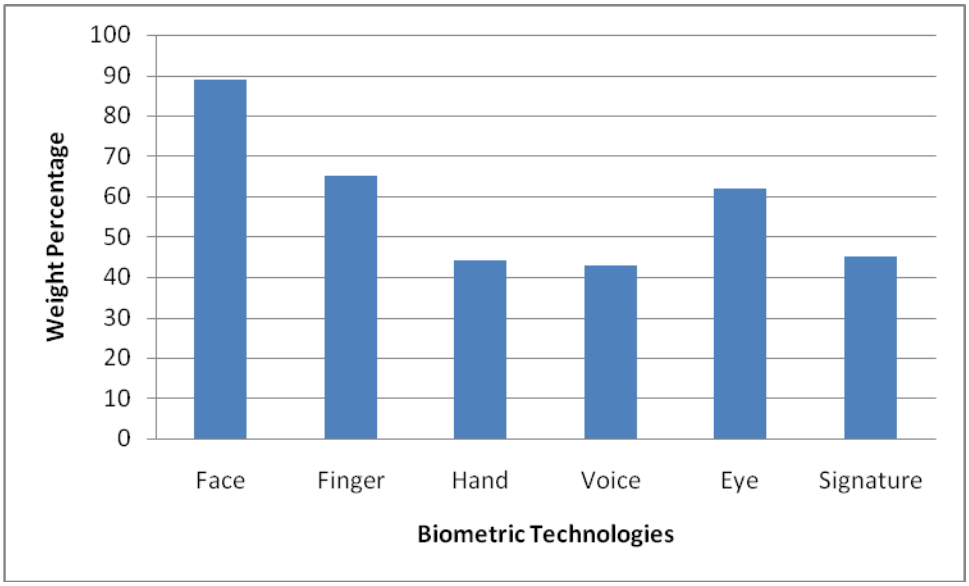


Figure 4.6: Comparison of various biometric features and their weighted percentage.

Receiver Operating Charactristic

In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). The ROC plot is obtained by graphing the values of FAR and FRR, changing the variable simplicity. (Adegun et al, 2014).

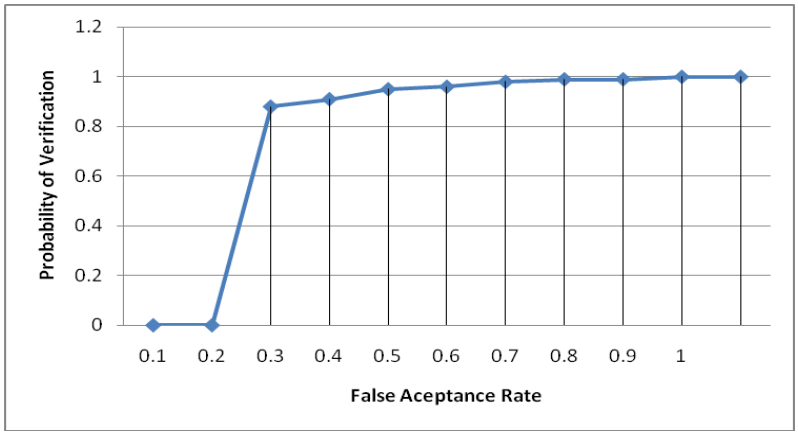


Figure 4.7 Receiver Operating Characteristic

4.2 Integration

Integration refers to the practice of combining individually tested software components into an integrated whole (Carnegie, 2012). It marks the end of the SDLC between module development and system integration testing.

4.2.1 Method of integration

Vertical Integration was preferred and involves integration of subsystems (modules) according to their functionality and position in the software architecture. The benefit of this method is that the integration is performed quickly and involves only the necessary subsystems.

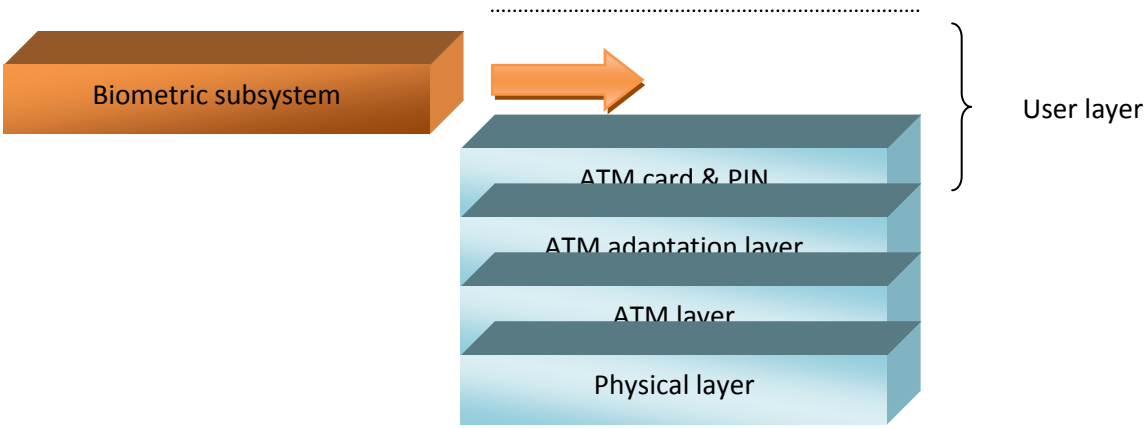


Figure 4.8 Receiver Operating Characteristic

Excellent software design approaches minimize the pairing between various components and maximize each components internal consistency with other subsystems. These designs are called

modular and they promote the ability to develop, change, and refine individual pieces independently (Melanchuk, 2012).

Independence between them shortens software development time and also reduces the total cost of supporting and maintaining the entire product.

4.3 Performance Evaluation

Our main objective in conducting this study is to determine whether experimental design and two-factor authentication modeling can be used in evaluating the performance of a facial recognition system, while still considering varying conditions during enrolment and probe-image and template matching.

The table below shows the effects of illumination and the time between capturing each image and their affect on face recognition performance.

Table 4.5: facial recognition verification performance

Class	False Acceptance Rate	False Rejection Rate
Same day with same illumination	2	0.4
Same day with different illumination	2	9
Different days	2	2

The head pose (pose angle), source of illumination, occlusion and image quality and resolution are our parameters in this set of experiments.

4.3.1 Factors of Evaluation

False accept rate (FAR), is a statistic used to measure biometric performance when performing the verification task. The percentage of times a face recognition algorithm, technology, or system falsely accepts an incorrect claim to existence or non-existence of a candidate in the database over all comparisons between a probe and gallery image. (Lucas D., 2006)

The false rejection rate, or FRR, is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system's FRR typically

is stated as the ratio of the number of false rejections divided by the number of identification attempts. (Webopedia)

The false rejection rate (FRR) is calculated as the percentage of scores from the same people that were classified as rejections. The false acceptance rate (FAR) is calculated as the percentage of scores from different people that were classified as acceptances (David Heseltine, 2005).

Relative Operating Characteristic (ROC): In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). The ROC plot is obtained by graphing the values of FAR and FRR, changing the variable simplicity. (Adegun et al, 2014).

Equal Error Rate (EER) describes the point at which genuine and imposter error rates are closest to zero. EER can be represented as a percentage with time/unit factors. It can be helpful as a first-order performance indicator for 1:1 verification systems. (USMA, 2012)

Failure to Capture Rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC (Adegun et al, 2014).

Template Capacity: It is defined as the maximum number of sets of data which can be input into the system (Adegun et al, 2014).

4.4 Conclusion

ATM access control has clearly shown that there exists a robust security specification that standardizes authentication in ATM machines. However, there are still a range of problems and pitfalls in identification and access control. We have keenly looked at the various security mechanisms of authentication available for identification and access control. We have analyzed passwords, PINs, smartcards and biometrics for their strengths and weaknesses. It is very important to have a strong non-intrusive access control mechanism to ensure that computerized resources are secure from unauthorized users. We have also looked at ease/difficulty of compromising these mechanisms and their cost of implementation. Future research should critically look at ethical hacking to expose other weaknesses of these access control mechanism.

5 DISCUSSIONS AND CONCLUSION

5.1 Experimental Results

We conduct experiments on the probe face images and stored data sets. For the experiment on the stored images, we select 89 test identities which are exclusive to our identity data set.
We indiscriminately select 11 mutually exclusive persons, against a database consisting of 150 images. The test task is to tell whether the probe images can be recognized from a database of multiple exclusive images of different individuals.
We use various kinds of data sets during the testing phase of the developed system. Errors are noted and used to make corrections. The corrections are also documented for future use and reference. The performance of face recognition can be measured with the help of the following factors.

Table 5.1: Performance evaluation of face recognition

	# Images	Highest Score	# Hits	# Repeats	# False Positives
1st Test	11	88	2	2	0
2nd Test	10	79	2	1	1
3rd Test	8	82	2	0	0
4th Test	8	86	2	1	0
5th Test	7	80	2	0	0
6th Test	7	88	2	0	0
7th Test	7	85	2	2	0
8th Test	6	89	2	2	0
9th Test	6	87	2	1	1
10th Test	6	83	2	0	0
11th Test	6	88	2	1	0
…	…	…	…	…	…

Face recognition needs to be advanced to overcome instabilities due to variable illuminations, face expressions, poses and occlusion. 150 face images from 89 individuals have been used to train face the recognition algorithm and testing the system`s performance. Most of the images in the database are not sufficiently annotated with the exact illumination angle, face expressions, pose angle, and illuminant color. We carried out tests which included images in the database

being matched with probe images from several individuals in different and exact capture environments. In the table above, we report the experimental results of face recognition performed using correlation matching and principal component analysis under various environmental conditions.

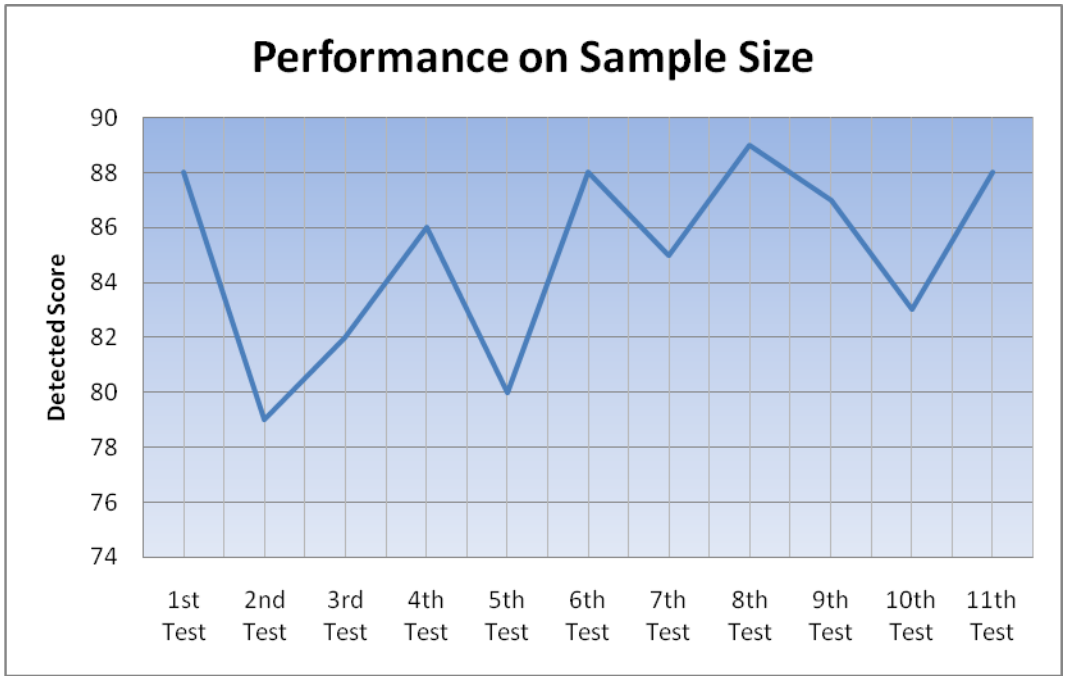


Figure 5.1: Relationship between sample size and detected score

Table 5.2: The impact of environmental changes and facial variations on the performance of face recognition

	# Images	Highest Score	Comments
1st Test	5	88	pose, illumination, occlusion and ***expression***
2nd Test	5	79	pose, illumination, ***occlusion*** and expression
3rd Test	5	75	***pose***, illumination, occlusion and expression
4th Test	5	72	***pose***, illumination, ***occlusion*** and ***expression***
5th Test	5	80	pose, ***illumination***, occlusion and expression
6th Test	5	65	***pose, illumination, occlusion*** and ***expression***
7th Test	5	85	pose, illumination, ***occlusion*** and ***expression***
8th Test	5	76	***pose***, illumination, occlusion and ***expression***
9th Test	5	84	pose, ***illumination***, occlusion and ***expression***
10th Test	5	83	pose, ***illumination, occlusion*** and expression
11th Test	5	78	***pose***, illumination, ***occlusion*** and expression
…	…	…	…

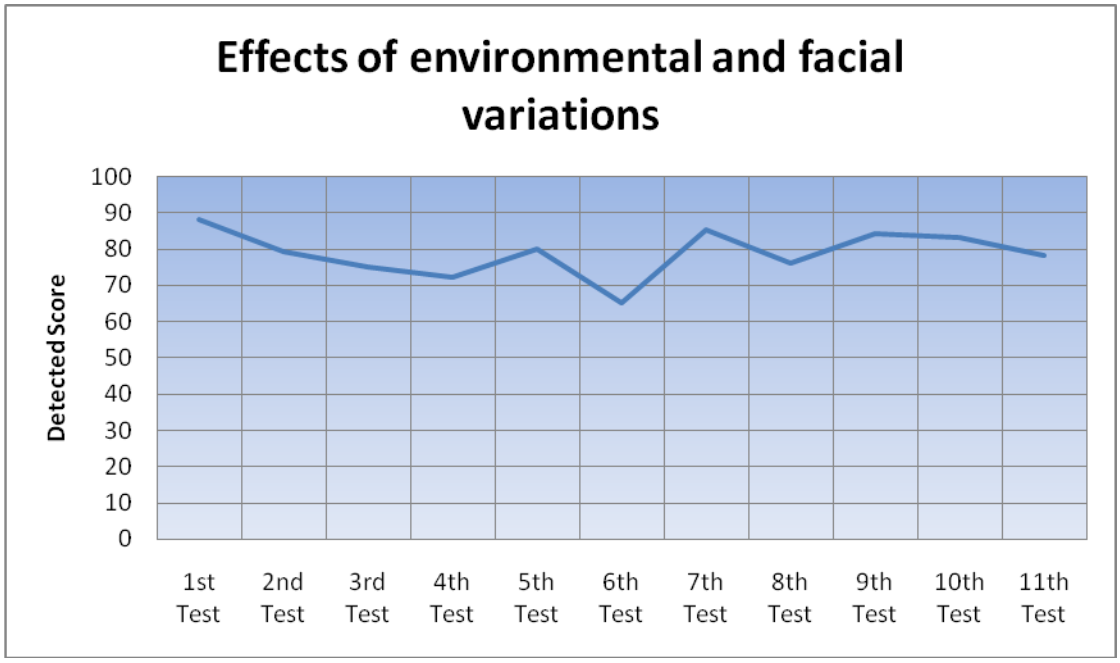


Figure 5.2: Effects of environmental and facial variations on performance

5.2 Improvements

In our experiments with neural networks, we used various samples and introduced a threshold which allowed us to accept or reject decisions and output. It allowed us to improve the

recognition performance of our model by considering all the outputs. It calculates the Euclidean distance between the best/perfect and real output for recognized person. When this distance is lower than the threshold we reject that person; otherwise the person is accepted.
Performing face recognition tests on a laptop with 1.3 Megapixel camera produced by Hp Compaq, using the Dummy Model with photos or videos of some users, we have been able to pass the User Authentication Based on Face Recognition and log into user accounts on model without much difficulty.

5.3 Result estimation

Below are results of the tests on the Dummy Model performing on an ATM application:

- Brute Force: attempting to bypass authentication using several face images.
- No Brute Force: attempting to bypass authentication using an arbitrary face image taken from a customer.
- High: easily bypassed
- Medium: rather difficult to bypass
- Low: cannot be bypassed at all

Table 5.3: Estimation of attack

	Face Recognition	PIN
Brute Force	Low	High
No Brute Force	-	Medium

In order to build a threat-resistant ATM security system, we need to identify the requirements of securing the services rendered by the machine. Below are the general requirements for an ATM security system:

1. Authentication: The user is the one he/she claims to be.
2. Confidentiality: Only authorized users can access the content of the data.
3. Integrity: The data is modified by legitimate users.
4. Non-repudiation: A user cannot deny that he/she has accessed a service or data.

The table below summarizes the mapping between the security objectives and the threats.

Table 5.4: Mapping between the security objectives and the threats

Objectives	**Generic Threats**						
	Masquerade	Eavesdropping	Unauthorized Access	Corruption or Loss of Data	Repudiation	Forgery	Denial of Service
Confidentiality	yes	yes	yes	--	--	--	--
Data Integrity	yes	--	yes	yes	--	yes	--
Accountability	yes	--	yes	--	yes	yes	--
Availability	yes	--	yes	yes	--	--	yes

5.4 Conclusion

Face recognition is a security measure in the field of computer vision, image analysis and pattern matching that is rather challenging to implement in systems to heighten system security and to curb unauthorized access. It has drawn much attention over the last few years because of its promising security features and its ability to be applied in various domains such as ID systems, voting systems, Automatic Teller Machines just to mention a few.

Past research in this field over the last few years have shown good progress and the results obtained so far shows that current facial recognition systems have reached acceptable and reasonable security threshold value while under operation in dynamic conditions and environments.

5.5 Challenges

It has been challenging for researchers to design an ideal face recognition system that can perform adequately under various constrained conditions commonly encountered while under operation in practical life. Cost to users of the technology has been a concern. The cost of a finger print scanner is relatively low while that of a retina scanner is extremely expensive.

5.6 Future Research

According to Michael Kraus, 2012, future developments of facial recognition should be able to detect human faces under any constrained conditions while upholding efficiency and accuracy. It should also be able to learn new faces and determine gender or facial expressions, and should also be able to deal with a range of aspects other than full frontal views.

5.7 Recommendations for face recognition

The accuracy of face recognition depends heavily on the quality of a face image during enrollment, as it influences the quality of the face template. The basic requirements of face recognition applications include the following:

5.7.1 Cameras and Images

1. It is recommended that Similar quality cameras are used during enrollment and identification processes. Also recommended that the same model of the camera is used.
2. A minimal distance of 50 pixels is recommended between the eyes for a face on image or video stream during the extraction of the face template.
3. A minimal camera resolution of 640 x 480 pixels is recommended for face enrollment and recognition.
4. Mirrored face images are not recommended as face recognition will fail if a non-mirrored image is used during face recognition.
5. It is recommended that several images be used during enrollment because it improves facial template quality. This increases both the quality of recognition and reliability.

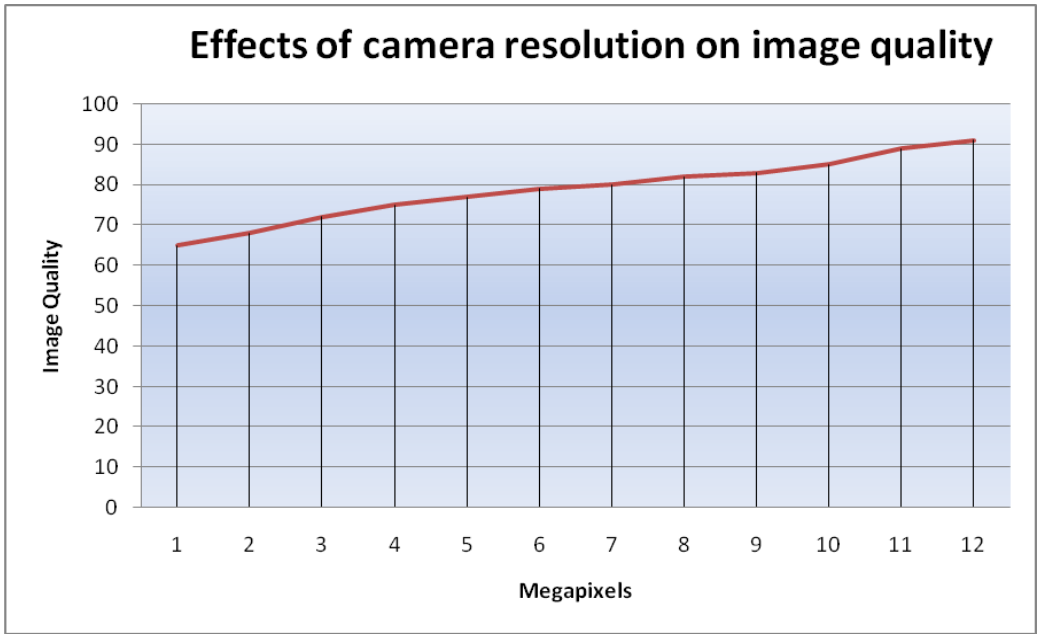


Figure 5.4: Effects of camera resolution on performance

5.7.2 Lighting

Lighting conditions should be controlled. Both direct frontal and diffused light are recommended as they allow equal lighting distribution on each side of the face and from top to bottom with no significant shadows within the face region.

5.7.3 Face Posture

- Head tilt: The face recognition engine can tolerate ±180 degrees;

The fastest setting for sufficient near-frontal face images is ±15 degrees default value.

5.7.4 Facial Expression

It is recommended that a neutral face expression be assumed during enrollment. Non-neutral face expression is likely to affect the accuracy of recognition. Non-neutral face expressions may include: frowning, closed eyes, smile, raised eyebrows, etc.

5.7.5 Live Face Detection

A continuous stream of images or video is required for face extraction.

1. A minimum of 10 frames is required.

2. The primary focus of the frames should be one face.
3. It is also recommended to move the head closer or further from the camera for features to be extracted efficiently.

5.7.6 Hair, Makeup, Glasses, Beard

It is recommended that different images with different look variants are captured to assure the quality of recognition when part of face is obstructed by makeup, glasses or Moustache. There can be several enrollments with and without glasses, makeup or moustache to assure the best recognition quality for both cases.

APPENDIX 1: GLOSSARY OF TERMS

Attributed identifier: A piece of personal information such as name and national identification number

Biographical identifier: Acquired piece of personal information such as address or education certificates

Biometric characteristic: The use of biological and/or behavioral characteristic of an individual for identification and verification purposes

Biometric verification: Confirmation of an identification claim through comparison

Biometric feature: A biometric attribute used for comparison

Comparison: The process of comparing a biometric template with a database of stored templates in an attempt to make an identification or verification.

False accept rate (FAR) and false reject rate (FRR): A statistical approach used to measure the performance of biometrics while under operation

Identification: Matching of a probe image against a database

Training set: A set of face images used to train the face algorithm to detect and extract features from a face

Recognition: A descriptive term in biometric systems e.g. voice recognition or face recognition

Threshold: A numerical value used for decision making in biometric systems

APPENDIX 2: REFERNCES

1. *A. Pentland, B. Moghaddam, and T. Starner, Viewbased and modular eigenspaces for face recognition, in IEEE Conference on Computer Vision and Pattern Recognition, 1994.*
2. *Belhumeur, P.N. ; Hespanha, J.P. & Kriegman, D.J. (1997). Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection, IEEE Transactions (PAMI)*
3. *Blanz, V., Romdhani, S., Vetter, T. Face Identification across Different Poses Chris Skinner, 2010.*
4. *David W. Embley, Bernhard Thalheim(Eds.): Handbook of Conceptual Modeling, 2011.*
5. *Davies, G., Ellis, H., and Shepherd, J. (1977) Cue saliency in faces as assessed by the 'Photofit' technique.*
6. *Dimitri PISSARENKO, Eigenface-based facial recognition December 1, 2002 Donglin Liang, 1997. A Survey on ATM Security.*
7. *Fraser, I. H., Craig, G. L., and Parker, D. M. (1990) Reaction time measures of feature saliency in schematic faces.*
8. *Guthery S. and Jurgensen T.M. (2001): "Smartcard developer's kit", Macmillan technical publishing. ISBN 1-57870-027-2.*
9. *Handbook of Face Recognition by Stan Z. Li Anil K. Jain.*
10. *He, Y.; Zhao, L. & Zou, C. (2006). Face recognition using common faces method, Pattern Recognition.*
11. *Heseltine, "Face Recognition:Two-Dimensional and Three-Dimensional Techniques" September 2005*
12. *Jeff Johnson and Austin Henderson: Conceptual Models in a Nutshell , 2013*
13. *John D. Woodward, Jr., Christopher Horn, Julius Gatune, Aryn Thomas, "Biometrics, A Look at Facial Recognition," RAND, 2003.*
14. *Kyungnam Kim, "Face Recognition using Principle Component Analysis", Department of Computer Science, University of Maryland, College Park, USA,1990*
15. *L. Sirovich and M. Kirby, "A Low-Dimensional Procedure for the Characterization of Human Faces," J. Optical Soc. Am. A, 1987,*
16. *Lindsay I Smith, A tutorial on Principal Components Analysis, February 26, 2002.*
17. *M. Yang, D. J. Kriegman, and N. Ahuja, "Detecting Face in Images: A Survey", IEEE Trans. on PAMI, Vol. 24, No. 1, pp. 3458, Jan. 2002.*
18. *Matthew A. Turk, Alex P. Pentland, Face Recognition Using Eigenfaces, Proc. IEEE Conference on Computer Vision and Pattern Recognition: 586–591. 1991.*
19. *Michael Kraus, Face the facts: facial recognition technology's troubled past--and troubling future, The Free Library, 2002.*
20. *Moses MICHIRA, 2014. New crimes study in Kenya on Automatic Face and Gender Recognition, 2002.*
21. *R. Brunelli, T. Poggio. Face Recognition through Geometrical Features. Proceedings ECCV92, 1992*

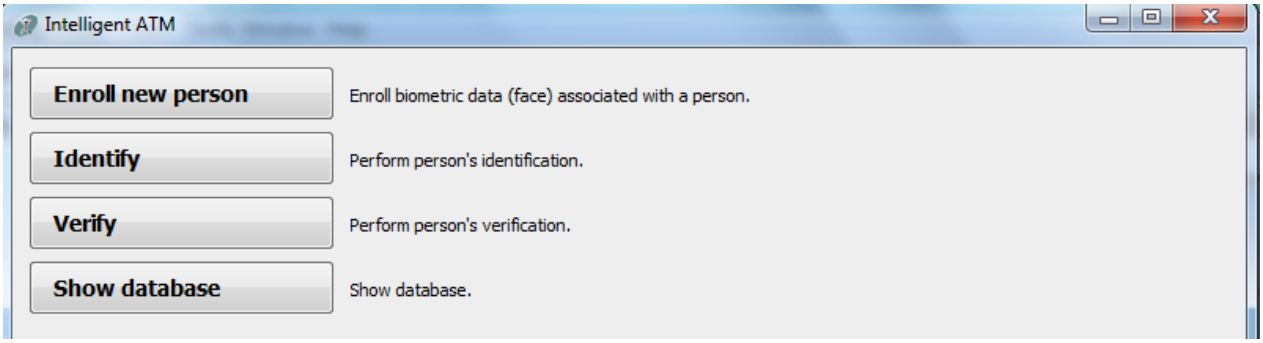
22. *Rapid application development (RAD). 2011. Rapid application development (RAD).*
23. *Rowley, H., Baluja, S., and Kanade, T., "Rotation Invariant Neural Network-Based Face Detection", Computer Vision and Pattern Recognition, pp. 38-44, 1998.*
24. *Ryan Johnson, Kevin Bonsor, "How Facial Recognition Systems Work," How Stuff Works, 2007.*
25. *Sadr, J., Jarudi, I. and Sinha, P. (2003). The role of eyebrows in face recognition, Perception,*
26. *Shang-Hung Lin, Ph.D.. "An Introduction to Face Recognition Technology", IC Media Corporation, 2000*
27. *Shang-Hung Lin, Ph.D.. "An Introduction to Face Recognition Technology", IC Media Corporation, 2000*
28. *Shepherd-Barron J. (2010):Working of automatic teller machine (ATM)*
29. *Smartcard alliance identity council (2007):Iidentity and smartcard technology.*
30. *Survey paper: Face Detection and Face Recognition By Hyun Hoi James Kim FRVT 2006 and ICE 2006 LargeScale Results*
31. *T. Kanade, "Computer Recognition of Human Faces." Basel and Stuttgart Birkhauser, 1977.*
32. *W. W. Bledsoe, "The model method in facial recognition," Panoramic Research Inc., Technical Report PRI15, Palo Alto, CA, 1964.*
33. *W. Zhao, R. Chellappa, A. Rosenfeld, P.J. Phillips, "Face Recognition A Literature Survey." ACM Computing Surveys, 2003.*
34. *Young, A. W., Hellawell, D. and Hay, D. C. (1987). Configurational information in face perception.*
35. *Journal, "THE CONTEXT OF DESIGN, 2014"*
36. *NIST/SEMATECH e-Handbook of Statistical Methods.*
37. *Adams, A. & Sasse, M. A. Users Are Not The Enemy. Communications of the ACM, (1999)*
38. *Florêncio, D. & Herley, C. A Large-Scale Study of Web Password Habits In Proc. WWW, 2007*
39. *Samzenpus,"Chip and Pin "Weakness" Exposed By Cambridge Researchers, 2012*
40. *M. Schumacher, E. B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns. Chichester, England: John Wiley & Sons Ltd, 2005*
41. *Machine Learning, Tom Mitchell, McGraw Hill, 1997.*
42. *An introduction to neural computing. Christos, Aleksander, I. and Morton, H. 2nd edition*

APPENDIX 3: RESEARCH QUESTIONS

1. Please indicate which one or more of the following biometric technologies you have used before.
   - o Fingerprint
   - o Iris recognition
   - o Voice recognition
   - o Face recognition
   - o Palm recognition
2. How often do you use biometric technology?
   - o Always
   - o Sometimes
   - o Never
   - o Often
   - o Seldom
3. When last has your organization investigated the use of biometric technology?
   - o More than 5 years ago
   - o Less than 12 months ago
   - o Between 3 to 5 years ago
   - o Never
   - o Between 1 to 2 years ago
4. Which biometric technologies has your organization investigated before? Mark ALL applicable.
   - o Fingerprint
   - o Face recognition
   - o Palm recognition
   - o Voice recognition
   - o Iris recognition
   - o None
5. Which biometric technologies is your organization still investigating? Mark ALL applicable.
   - o Fingerprint
   - o Face recognition
   - o Palm recognition
   - o Voice recognition
   - o Iris recognition
   - o None
6. Please indicate which one or more of the following biometric technologies are your organization using for client banking applications? Mark ALL applicable.
   - o Fingerprint
   - o Face recognition
   - o Retinal recognition
   - o Voice recognition
   - o Iris recognition
   - o None
7. How long has your organization been using this/these technology (ies) for client banking applications?
   - o More than 5 years ago
   - o Less than 12 months ago
   - o Between 3 to 5 years ago
   - o Never
   - o Between 1 to 2 years ago
8. Which banking channels use biometrics in your organization
   - o Internet Banking
   - o Community Banking
   - o ATM
   - o None
   - o Banking in the Branch
   - o Other. Give details……
9. In which banking channel do you think biometrics works well
   - o Internet Banking
   - o Community Banking
   - o ATM
   - o Other. Give details……
   - o Banking in the Branch
10. Please indicate which one or more of the following biometric types should be used for authentication in banking applications such as an ATM. Mark ALL applicable.
    - o Fingerprint
    - o Face recognition
    - o Retinal recognition
    - o Voice recognition
    - o Iris recognition
    - o None
11. My organization is a leader in setting world class trends like the use of biometric authentication for banking applications
    - o Strongly agree
    - o Neutral
    - o Strongly disagree
    - o Agree
    - o Disagree
12. IN CONCLUSION, do you support the use of biometrics as a security tool?
    - o Yes
    - o No

APPENDIX 4: USER MANUAL

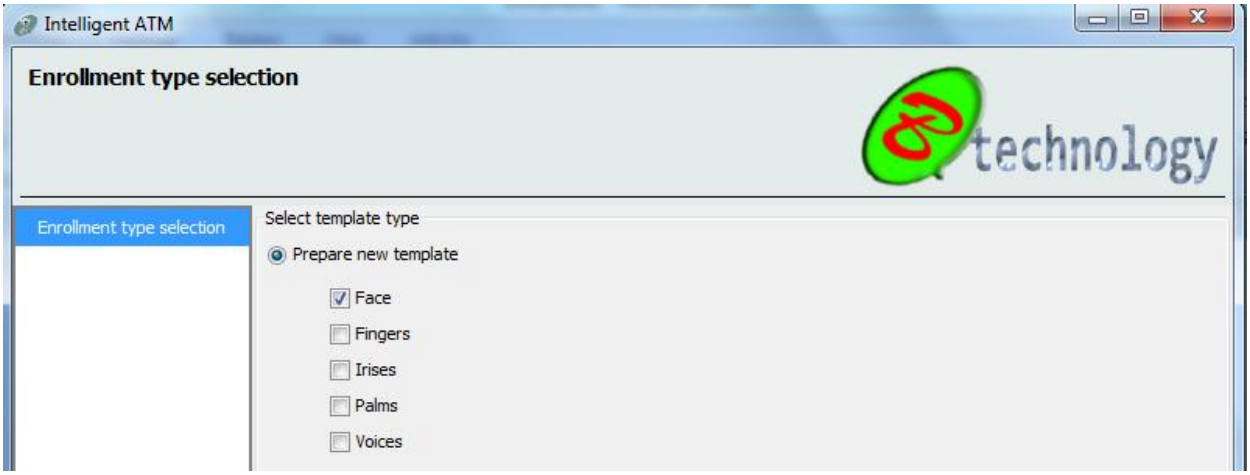
Enrolment sub module



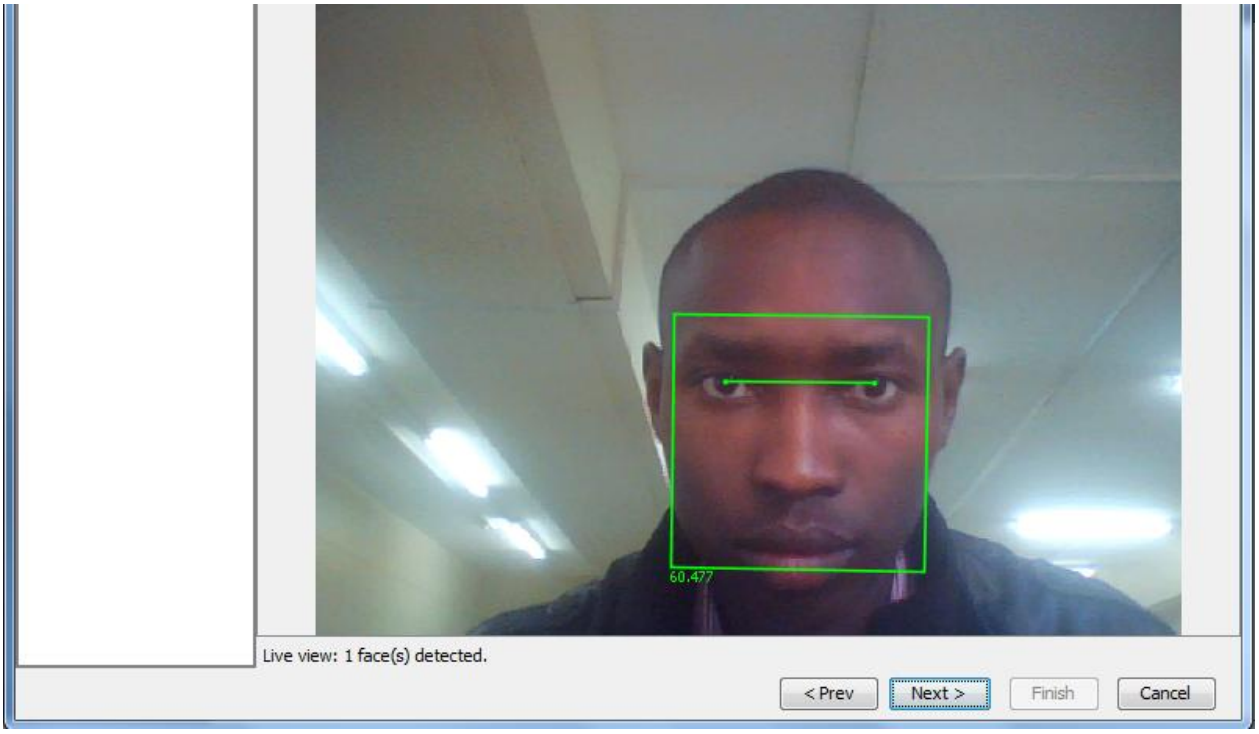
This is the dashboard that provides access to enrolment and identification modules.

```
package server.identification;
import java.io.File;
import server.ATMDialog;
import server.ATMThread;
import server.GlobalSettings;
import server.database.Customer;
import server.database.Face;
public class IdentifyByFace extends Identification {

	public IdentifyByFace(ATMThread aTMThreat) {
		super(aTMThreat);

	}
	public ATMDialog identify(ATMDialog data) {
    //Start of user code for Identification.identifyByNR
	if (state == 0) {
		state++;
		return new ATMDialog("Please look at the camera and press Capture\n","f","0");
	}
	Customer customer = null;
	String faceFile = GlobalSettings.getDataDir()+ File.separator
+String.valueOf(aTMThreat.getConNr())+".jpg";
	if (data.getReturnedInputFile(faceFile)) {
		Face face = new Face(faceFile);
		face.setUsedForTraining(false);
		customer = aTMThreat.getDatabase().getCustomerByFace(face);
	}
	if (customer == null) {
		state++;
```

```
                if (state >4)
                        return this.identifyFail();
                return new ATMDialog("Unknown face,\nPlease try again!","f","0");
        }
        else {
                return identifyPass(customer);
    //End of user code
        }
  }

}
```

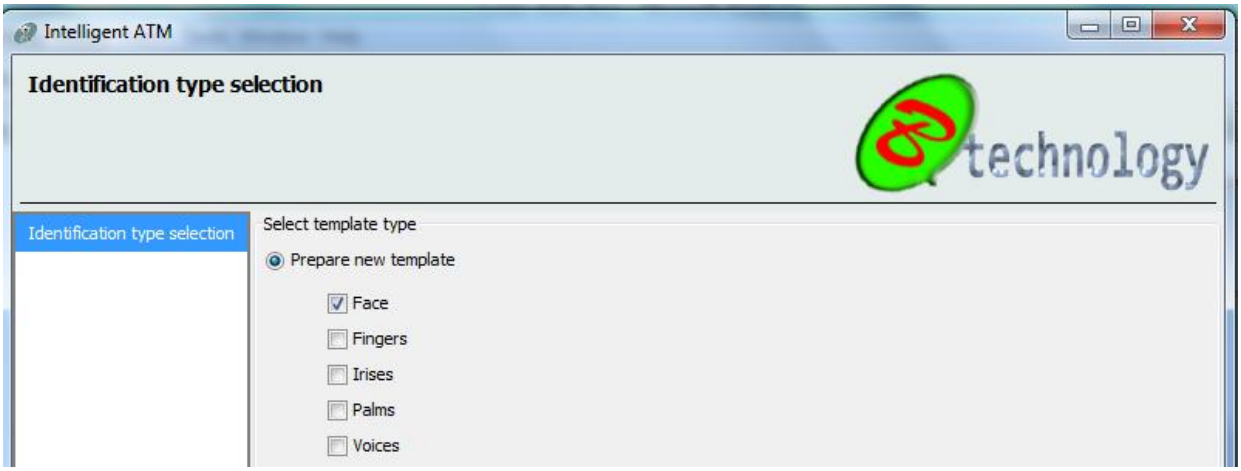


A number of biometric technologies can be used in identification or verification. Our area of research focus on face recognition.



Face image enrolment. The face charactristic used is the distance between the middles of the eyes.

Identification submodule



Face recognition will be checked; it is to be checked to perform the template matching.

```
package server.identification.eigenface;
import java.awt.image.BufferedImage;
import java.util.ArrayList;
import java.util.HashMap;
import server.GlobalSettings;
import server.database.FaceDatabase;
import server.database.Face; import de.offis.faint.global.Utilities;
import de.offis.faint.global.Utilities.SortableContainer;
```

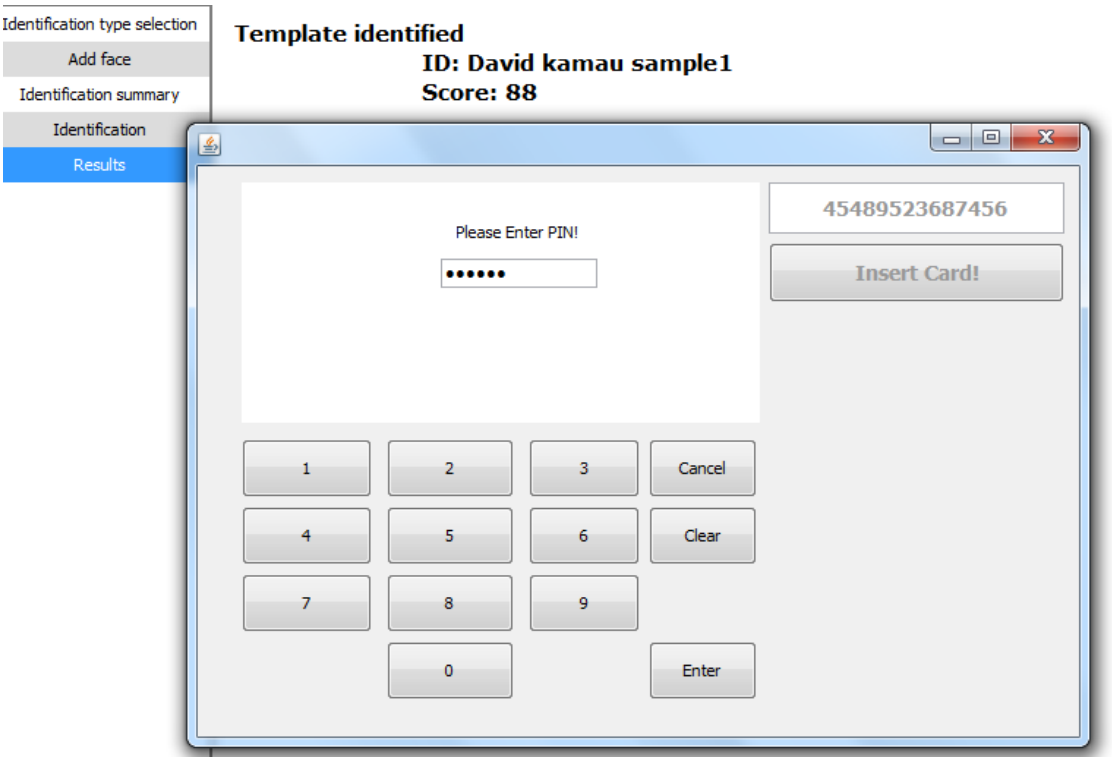
```
import de.offis.faint.gui.tools.InfoDialog;
public class EigenfaceRecognition  {
	FaceDatabase faceDB = null;
	// Constants
	private static final long serialVersionUID = 4547532707099091006L;
	protected final static int VECTORLENGTH = GlobalSettings.FACE_THUMBNAIL_SIZE.height *
GlobalSettings.FACE_THUMBNAIL_SIZE.width;

	// Settings
	protected Integer maxEigenfaces = null;
	protected Integer rebuildFaceSpace = null;
	protected boolean mirrorFaces = true;

	// Data
	private byte[] averageFace = null;
	private ArrayList<double[]> eigenFaces = null;
	protected int lastNumberOfTrainingImages = 0;

	// Transient elements
	protected transient boolean updateIsRunning = false;
	private transient EigenfaceBuilder eigenfaceBuilder = null;



	public EigenfaceRecognition (FaceDatabase faceDB) {
		this.faceDB = faceDB;
		//System.out.println("EigenfaceRecognition");
	}

	public synchronized HashMap<String, Integer> getRecognitionPoints(Face region) {
		//System.out.println("getRecognitionPoints1");
		//faceDB.printSize();
		// Ensure an instance of EigenfaceBuilder is present
		if (eigenfaceBuilder == null)
			eigenfaceBuilder = new EigenfaceBuilder(this);

		// Prepare first set of Eigenfaces (in same thread)
		/*if (averageFace == null )
			System.out.println("averageFace == null");
		if (eigenFaces == null )
			System.out.println("eigenFaces == null");
		*/

		if (averageFace == null || eigenFaces == null){
			eigenfaceBuilder.updateEigenfaces();
			if (averageFace == null){
				new InfoDialog(null, "<html>Not enough training images availble for
EigenfaceRecognition.<br>Please classify the first faces manually!</html>");
```

```
                        return new HashMap<String, Integer>();
                }
        }
        //System.out.println("getRecognitionPoints2");
        FaceDatabase db = faceDB;
        //faceDB.printSize();
        String[] names = db.getExistingAnnotations();

        BufferedImage unknownFaceImage =
region.toThumbnail(GlobalSettings.FACE_THUMBNAIL_SIZE);

        byte[] unknownFace = Utilities.bufferedImageToIntensityArray(unknownFaceImage);
        double[] unknownFaceWeight = this.getWeightForImage(unknownFace);

        // Mirrored region may increase recognition performance
        double[] unknownMirroredFaceWeight = null;
        if (this.mirrorFaces){
                byte[] mirroredFace = new byte[unknownFace.length];
                for (int i = 0; i < GlobalSettings.FACE_THUMBNAIL_SIZE.height; i++){
                        for (int j = 0; j < GlobalSettings.FACE_THUMBNAIL_SIZE.width; j++){
                                int elem = i * GlobalSettings.FACE_THUMBNAIL_SIZE.width + j;
                                mirroredFace[elem] = unknownFace[(i+1) *
GlobalSettings.FACE_THUMBNAIL_SIZE.width - j - 1];
                        }
                }
                unknownMirroredFaceWeight = this.getWeightForImage(mirroredFace);
        }

        HashMap<String, Integer> result = new HashMap<String, Integer>(      names.length);
        ArrayList<SortableContainer<Face>> bestHits = new ArrayList<SortableContainer<Face>>();
        for (String name : names) {
                Face image = null;
                Face[] regionsForName = db.getRegionsForFace(name);

                if (regionsForName != null) {
                        double minDist = Double.MAX_VALUE;

                        for (int i = 0; i < regionsForName.length; i++) {

                                if (regionsForName[i] != null && regionsForName[i] != region &&
regionsForName[i].isUsedForTraining()) {

                                        byte[] knownFace = Utilities

        .bufferedImageToIntensityArray(regionsForName[i]

        .toThumbnail(GlobalSettings.FACE_THUMBNAIL_SIZE));
```

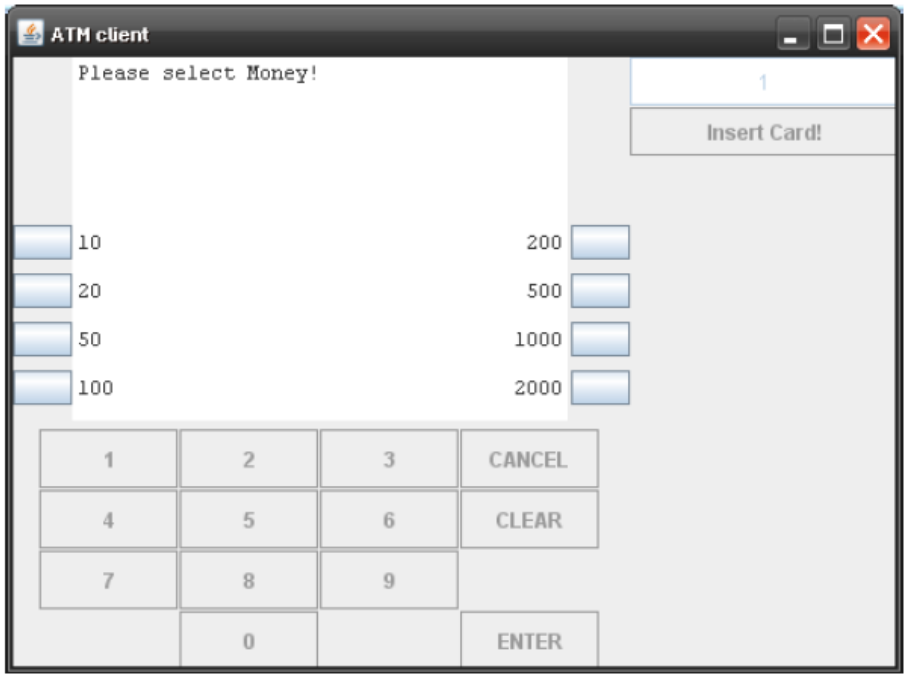
```
                                                double[] knownFaceWeight =
this.getWeightForImage(knownFace);

                                                double distance =
this.getDistanceBetweenWeights(knownFaceWeight, unknownFaceWeight);

                                                if (unknownMirroredFaceWeight != null) {
                                                        distance = Math.min(distance,
getDistanceBetweenWeights(knownFaceWeight, unknownMirroredFaceWeight));
                                                }

                                                if (distance < minDist) {
                                                        minDist = distance;
                                                        image = regionsForName[i];
                                                }
                                        }
                                }

                                // Map distance to interval [0, 100]
                                Integer points = (int) Math.max(0, 100 - Math.round(minDist * 0.2f));
                                result.put(name, points);

                                if (image != null && points != 0){
                                        bestHits.add(new SortableContainer<Face>(image, points));
                                }
                        }
                }
                // Prepare upcoming set of Eigenfaces in second thread.
                //eigenfaceBuilder.updateEigenfacesInBackground();
                return result;
        }

        protected double[] getWeightForImage(byte[] image){

                short[] distanceFromAverageFace = new short[VECTORLENGTH];
                for (int i = 0; i< distanceFromAverageFace.length; i++){
                        distanceFromAverageFace[i] = (short)(((short) image[i] & 0xFF) - ((short)
this.averageFace[i] & 0xFF));
                }
                double[] result =  new double[this.eigenFaces.size()];
                for (int i = 0; i < result.length; i++){
                        result[i]=0;
                        for (int j = 0; j<this.eigenFaces.get(i).length;j++){
                                result[i]+= this.eigenFaces.get(i)[j] * distanceFromAverageFace[j];
                        }
                }
                return result;
        }
```

```
	protected double getDistanceBetweenWeights(double[] weightA, double[] weightB){
		double result = 0;
		for(int i = 0; i<weightA.length; i++){
			result+= Math.abs(weightA[i] - weightB[i]);
		}
		return result/weightA.length;
	}
	protected byte[] getAverageFace() {
		return averageFace;
	}

	protected ArrayList<double[]> getEigenFaces() {
		return eigenFaces;
	}
	protected byte[] getFaceReconstruction(double[] weight){
		double [] temp = new double[VECTORLENGTH];

		for (int i = 0; i< weight.length; i++){
			for (int j = 0; j < temp.length; j++)
				temp[j] += weight[i] * this.eigenFaces.get(i)[j];

		}
		for (int j = 0; j < temp.length; j++)
		{
			temp[j] += averageFace[j] & 0xff;
		}
		byte[] image = new byte[VECTORLENGTH];
		for (int i = 0; i < image.length; i++){
			int value = (int) Math.max(0, Math.min(Math.round(temp[i]), 255));
			image[i] = (byte)(value & 0xff);
		}
		return image;
	}
	protected synchronized void updateData(byte[] averageFace, ArrayList<double[]> eigenFaces, int
numTrainingImages){
		this.lastNumberOfTrainingImages = numTrainingImages;
		this.averageFace = averageFace;
		this.eigenFaces = eigenFaces;
	}
	public String toString(){
		return getName();
	}
	public String getName() {
		return "Eigenface Recognition";
	}
	public String getDescription() {
		return "<p>This Plugin is an implementation of the Eigenfaces approach implemented entirely in
Java. Note: The recognition performance relies heavyly on the training sets of faces.</p>";
```

```
        }

        public String getCopyrightNotes() {
                return "<p>Malte Mathiszig 2007. Functions to calculate Eigenvalues of a matrix as found in Java Matrix Package (JAMA) are used. JAMA is a cooperative product of The MathWorks and the National Institute of Standards and Technology (NIST).</p>";
        }

        public FaceDatabase getFaceDatabase () {
                return faceDB;
        }
}
```



If the template is identified, the user is allowed to access financial services or otherwise denied.



The authenticated customer gets now access to the financial service.