A FACE-BASED ATM IDENTIFICATION SECURITY MODEL FOR FINANCIAL INSTITUTIONS

BY

FRED, HENRY KAYODE

DEPARTMENT OF MATHEMATICS
AHMADU BELLO UNIVERSITY, ZARIA
NIGERIA

DECEMBER, 2011

A FACE-BASED ATM IDENTIFICATION SECURITY MODEL FOR FINANCIAL INSTITUTIONS

BY

FRED, HENRY KAYODE
M.Sc/Sci/012894/2007-2008

A THESIS SUBMITTED TO THE
POSTGRADUATE SCHOOL,
AHMADU BELLO UNIVERSITY, ZARIA
NIGERIA

IN PARTIAL FULFILMENT FOR THE AWARD
OF MASTERS OF SCIENCE IN
COMPUTER SCIENCE

DEPARTMENT OF MATHEMATICS
AHMADU BELLO UNINIVERSITY, ZARIA
NIGERIA.

DECEMBER, 2011

DECLARATION

I declare that the work in the thesis entitled *A Face-based ATM Identification Security Model for Financial Institutions'* has been performed by me in the Department of Mathematics under the supervision of Professor S.O Adewale and Dr O. Choji.

The information derived from the literature has been duly acknowledged in the text and a list of references provided. No part of this thesis was previously presented for another degree or diploma to the best of my knowledge in any University.

Fred, Henry Kayode	_____	_____
Name of Student	**Signature**	**Date**

CERTIFICATION

This thesis entitled *A FACE-BASED ATM IDENTIFICATION SECURITY MODEL FOR FINANCIAL INSTITUTIONS* by FRED, Henry Kayode (Reg. No.: M.Sc/Scie/012894/2007-2008) meets the regulations governing the award of Master of Science degree of Ahmadu Bello University, Zaria and is approved for its contribution to knowledge and literary presentation.



26/06/2012

Prof. O.S. Adewale — **Date**
Major Supervisor

_____ _____

Dr O Choji — **Date**
Co-Supervisor

_____ _____

External Examiner — **Date**

_____ _____

Dr. B. Sani — **Date**
Ag. Head of Department

_____ _____

Prof. A.A. Joshua — **Date**
Dean of Postgraduate School

DEDICATION

I dedicate this work to the glory of God, the Alpha, and the Omega.

ACKNOWLEDGEMENT

I appreciate the Almighty God for His wisdom and strength He bestowed on me to make this project work successful.

I would like to really acknowledge the supervision of my major supervisor, Prof. O. S Adewale and my minor supervisor Dr. Choji. My thanks go to the Head of Department and the entire members of Department of Mathematics, ABU, Zaria.

Thanks to Mr. Ibrahim Abdullahi , Mr. A Onifade, Dr Obiniyi, Dr A.Mohammed and all my Masters' degree Classmates; May God continue to strengthen you all (amen).

ABSTRACT

There is the need for additional strengthening of security system in the present days Automatic Teller Machine (ATM) in banks. The current card and pin in use is not good enough to ensure the identity of the customer given the existing high rate of fraud. This very high rate of fraud care be minimised by an additional biometric system. A face recognition system is thereby proposed, implemented and tested in this thesis study. A face classification method that uses the eigenfaces approach with principal component analysis is integrated in the proposed system. The proposed system is designed to be able to capture and recognise faces within certain environmental condition. Experimental results are given to demonstrate the viability of the proposed face recognition system.

TABLE OF CONTENTS

Declaration - - - - - - - - - - iii

Certification - - - - - - - - - - iv

Dedication - - - - - - - - - - v

Acknowledgment - - - - - - - - - vi

Abstract - - - - - - - - - - vii

Table of Contents - - - - - - - - -ix

List of Figures - - - - - - - - -xiii

List of Appendices - - - - - - - - - xiv

List of Abbreviation - - - - - - - - - xv

CHAPTER ONE

1.0 Introduction - - - - - - - - - 17

1.1 General Background of the Study - - - - - - 17

1.2 Research Motivation - - - - - - - 21

1.3 Research Objectives - - - - - - - 24

1.4 Research Methodology - - - - - - - 24

1.5 Expected Contribution to Knowledge - - - - - - 25

1.6 Organisation of the Rest of the Thesis - - - - - 26

CHAPTER TWO

2.0 Literature Review - - - - - - - - 27

2.1 Introduction - - - - - - - - - 27

2.2 Frauds at ATMs - - - - - - - - - 31

2.3 Biometrics - - - - - - - - - - -33

2.3.1 Enrolment, Template, Algorithm, and Verification - - - -43

2.3.2 FAR, FRR, and FTE - - - - - - - -44

2.3.3 A System Model - - - - - - - - - 45

2.3.4 Data Collection - - - - - - - - - 45

2.3.5 Transmission - - - - - - - - - 47

2.3.6 Signal Processing - - - - - - - - - 48

2.3.7 Storage - - - - - - - - - -51

2.3.8 Decision - - - - - - - - - - 52

2.3.9 Applications of Biometrics - - - - - - - 53

2.3.10 Biometric Characteristics - - - - - - - -56

2.4 Strong Authentication in E-Banking - - - - -57

2.4.1 The Importance of a Two-Factor Authentication in e-Banking - -57

2.4.2 What is Strong User Authentication? - - - - - -58

2.4.3 Two-factor Authentication and non-Repudiation - - -59

2.4.4 Why is Strong Authentication needed in e-Banking? - - -62

2.4.5 The importance of Risk Assessment - - - - -65

2.4.6 Positive Return on Investment (ROI) - - - - -69

2.5 Identity Management - - - - - - - -69

2.5.1 Identity Management Models - - - - - - -70

2.5.2 Isolated Identity Management - - - - - - -71

2.5.3 Federated Identity Management - - - - - - -71

2.5.4 Centralised Identity Management - - - - - -72

2.5.5 Authentication and Authorisation - - - - - -72

2.6 Approaches to Face Recognition - - - - - - -73

2.6.1 Template Based Methods - - - - - - - - -77

2.6.2 Statistical Approaches - - - - - - - - -78

2.6.3 Neural Network Based Approaches - - - - - -78

2.6.4 Hybrid Approach - - - - - - - - - -81

2.6.5 Geometry Feature Based Methods - - - - - -82

2.6.6 Other Approaches - - - - - - - - - - 84

2.6.7 Face recognition using Principal Component Analysis - - - - 86

CHAPTER THREE

A FACE–BASED ATM IDENTIFICATION SECURITY MODEL

3.1 Face Recognition using Principal Component Analysis - - -90

3.1.1 Eigen-Faces for Recognition - - - - - - - -90

3.2 Architecture of a Face-Based Secure ATM Identification Security System

- - - - - - - - - - - -98

CHAPTER FOUR

SYSTEM IMPLEMENTATION

4.1 Introduction - - - - - - - - - -102

4.2 How the system works - - - - - - - - -103

4.3 Development Environment- - -- - - - - 108

4.4 Result and Discussion - - - - - - -109

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary - - - - -111

5.2 Conclusion - - - -112

5.3 Recommendation - - - - -113

5.4 Future Work - - - - -113

REFERENCES- - - - - - - - - -

APPENDIX A - - - - - - - - -

APPENDIX B - - - - - - - - -

LIST OF FIGURES

1. Fig 2.1: Biometric Traits that can be used for Authenticating An Individual - - - - - - - - - - 39
2. Fig 2.2: Generic Biometric Authentication System - - - - 46
3. Fig 2.3: Biometric system being deployed in various applications - 55
4. Fig 2.4: Summary of approaches to face recognition- - - - 77
5. Fig. 3.1: Formation of the faces vector from the faces image - - - 92
6. Fig 3.2: The face space (u_1 and u_2 are the eigenfaces)- - - - 96
7. Fig 3.3: Main modules in a face identification system - - - 98
8. Fig 3.4: Unified Modelling Language sequence diagram of the recognition process. - - - - - - - - - - 99
9. Fig 4.1: ATM Security Model - - - - - - 102
10. Fig 4.2: Identification process - - - - - - 107
11. Fig 4.3: Pictures used for face recognition - - - - 108- 109

LIST OF APPENDICES

APPENDIX A: CREATING AND RUNNING THE PROJECT WORK.

APPENDIX B: SOURCE CODES

LIST OF ABBREVIATIONS

Jpeg	- Joint Photographic Experts Group
ATM	- Automatic Teller Machine
PCA	- Principal Component Analysis
ROI	- Return on Investment
FAR	- Far Acceptance Rate
FRR	- False Rejection Rate
FTE	- Failure to Enrol
EFT	- Electronic Fund Transfer
PIN	-Personal Identification Number
HTML	- Hyper Text Mark-up Language
ICSA	- International Computer Security Association
SSL	- Secure Socket Layer
PKI	- Public Key Infrastructure

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

An automated teller machine (ATM) is a computerised telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier or bank teller.

On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smart card with a chip, which contains a unique card number and some security information such as an expiration date or card validation code. Authentication is provided by the customer entering a personal identification number (PIN).

Using an ATM, customers can access their bank accounts in order to make cash withdrawals or deposits, credit card cash advances, and check their account balances as well as purchase prepaid cellphone credit. If the currency being withdrawn from the ATM is different from that which the bank account is denominated in (e.g. withdrawing US Dollars from a bank account containing Nigeria Naira), the money will be converted at a wholesale exchange rate. Thus, ATMs often provide the best possible exchange rate for foreign travellers (Schlichter, 2007), and are heavily used for this purpose as well.

ATMs are known by various other names including automatic banking machine or automated banking machine (particularly in the United States), automated transaction

machine, cash point (particularly in the United Kingdom), money machine, bank machine, cash machine, hole-in-the-wall, autoteller (after the Bank of Scotland's usage), *cash line machine* (after the Royal Bank of Scotland's usage), *MAC Machine* (in the Philadelphia area), *Bankomat* (in various countries particularly in Europe and including Russia), *Multibanco* (after a registered trade mark, in Portugal), *Minibank* in Norway, *Geld Automaat* in Belgium and the Netherlands, and *All Time Money* in India.

ATMs are placed not only near or inside the premises of banks, but also in locations such as shopping centres/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather. These represent two types of ATM installations: on and off premise. On premise (in branch or in lobby) ATMs are typically more advanced, multi-function machines that complement an actual bank branch's capabilities and thus more expensive. Off premise (offsite) machines are deployed by financial institutions and also ISOs (Independent Sales Organisations) where there is usually just a straight need for cash, so they typically are cheaper mono-function devices.

Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account or in the country where their accounts are held (enabling cash withdrawals in local currency). ATMs rely on authorization of a financial transaction by the card issuer or other authorizing institution via the communications network. This is often performed through an ISO 8583 messaging system (Kumar, 2010).

Many banks charge ATM usage fees. In some cases, these fees are charged solely to users who are not customers of the bank where the ATM is installed; in other cases, they apply to all users.

ATMs typically connect directly to their host or ATM Controller via either **A**symmetric Digital Subscriber Line (ADSL) or dial-up modem over a telephone line or directly via a leased line. Leased lines are preferable to Plain Old Telephone Service (POTS) lines because they require less time to establish a connection. Leased lines may be comparatively expensive to operate versus a POTS line, meaning less-trafficked machines will usually rely on a dial-up modem. That dilemma may be solved as high-speed internet Virtual Private Network (VPN) connections become more ubiquitous. Common lower-level layer communication protocols used by ATMs to communicate back to the bank include Systems Network Architecture (SNA) over Systems Development Life Cycle (SDLC), TC500 over Async, standard suite of protocols used for packet switching across computer networks. (X.25), and Transmission Control Protocol/Internet Protocol (TCP/IP over Ethernet).

In today's corporate environment, the need exists to ensure that only authorised individuals or customers gain access to critical devices or services offered. With the availability of ready to use "sniffers" and access code (password/PIN) cracking tools, the standard username/password or PIN combination may no longer be adequate to withstand the test of secure authentication.

Other means of discovering password and/or PIN are aided by bad habits. Many customers and users in general use easy-to-guess combinations, compromise their PIN make infrequent changes, and often write their password or PIN down and leave it in conspicuous places, for example stuck to the computer monitor. Some customers not only never change their password or PIN, but also assign the same value to all their online access codes and even to their ATM cards.

Many organisations are depending on sophisticated and complex networks that have become one of the most important channels to do business, It is becoming an accepted norm that using a single factor authentication method may not be adequate to serve the growing high-risk e-business marketplace from a security point of view.

Authentication, however, cannot exist in a vacuum. It must be part of a security framework. The four security control objectives that address an adequate security framework are: (i) identification and authentication - to prove identity and allow access to assets; (ii) integrity - ensure that data was changed by the authorised person and that no unauthorised changes have been made; (iii) confidentiality - restricting data access to the people authorised to see it; (iv) non-repudiation - one may not deny his/her actions; (v) availability; and access control.

Typically an ATM has two types of devices: (i) input devices, which are card reader and keypad; and (ii) output devices, consists of display monitor screen, cash dispenser, receipt printer and speaker. The limit in usage is greatly being hurdled in using keyboard for entering password. Biometric technology can be used in breaking the hurdles of

keypad usage to help the rural and illiterate people. In biometric technology, the identity of user will be recognised by biological phenomena of human body. Biological structures and actions of different body parts of human body ranges from fingerprint, DNA, gait recognition, face recognition to voice recognition, can be used in biometric ATMs.

Since biometric technology can be used in the place of PIN codes in ATMs, its benefits mostly accrues to rural and illiterate masses who find it difficult to use the keypad of ATMs. Such people can easily put their face at the box available at ATMs machines and proceed with their transactions.

In computerised world, people are forced to remember several passwords. Biometric technology will help users by restricting their headache to remember another password of ATMs. In the usage of conventional ATMs, if you have forgotten password and given the trial of hitting wrong password for more than three times, the chances are there that your account will be blocked for ATM usage for that day. Besides, generating a new password request also puts burden on ATM users.

Biometric technology provides strong authentication, as it uses the unique features of body parts. This may help in reducing the chances of ATM frauds. Therefore, a robust and resilient authentication is imperative for all communications traffic between the ATM and the transaction processor for financial institutions engaging in any form of electronic banking or commerce.

1.2 Research Motivation

ATM is an automated device that provides the customers of a financial institution with the ability to perform financial transactions without the need for a human clerk or bank teller.

Crime at ATMs has become a national challenge to not only customers, but also bank operators. Security measures at banks can play a critical and paramount role in preventing attacks on customers. These measures are of great importance if banks must live up to the standard expected of them of providing a safe and secure banking environment for their customers.

The ATM is a terminal provided by bank or other financial institutions which enables the customer to withdraw cash to make a balance enquiry, to order a statement, to make a money transfer, or deposit cash. The ATMs are basically self-service banking terminals and are aimed at providing fast and convenient service to customers.

Some of the new generations of ATMs are able to cash a check to the kobo dispense traveller's cheques and postage stamps, perform stock transfers, print discount coupons, issue phone cards, and even sell concert tickets. Customers are grateful for these ATM features but they are also very concerned with ATM crime and safety.

ATMs are generally designed for through-the-wall operations as well as for use in lobbies. The Banker's magazine, September, 1983, indicated that the ATMs provided convenient bank access to customers accounts 24 hours a day, seven days a week

including public holidays. The lobby machines which are installed in the banking lobbies are only operational during banking hours. Essinger (1987) indicated that "ATM machines allow bank customers who have been issued with a card and a four- or six-digit secret number known as a PIN number (Personal Identification Number) to perform their own banking transactions". The plastic card contains a magnetic stripe or a chip that contains a unique card number and some security information, such as an expiration date and card validation code (cvc).

Kalakota and Whinston (2001), mentioned that the financial services industry has been through structural and operational changes since the mid-1990s, by innovative use of new information technology, electronic commerce. Hamelink (2000), indicated that the perceived cost reductions is the moving force behind the ongoing changes in banks .The implementation of the new technology has its benefits, associated risks and new challenges.

Rizal Commercial Banking Corporation (RCBC) (2007), mentioned that authentication of the user is provided by the customer entering a PIN. Furthermore, customers transacting on these ATMs are guided by instructions displayed on the video screens. These ATMs normally dispense two or more denominations of paper money. Customer's advice slips are automatically printed and dispensed except for balance enquires. All deposits have to be accounted for by the bank staff, before they are credited to customers' accounts.

Marcia Crosland (2010) indicated that aside from revenue generation and cost savings, ATMs are becoming the face of many financial institutions. For many consumers, ATMs

are becoming the only interaction they have with their banks. In addition, ATMs are also becoming a competitive mark for many banks. Therefore, it is imperative to ensure that the customer's experience with the ATM is safe and secure.

Fenton (2000) mentioned that over the past three decades, consumers have come to depend on and trust the ATM to conveniently meet their banking needs. In recent years there has been a proliferation of ATM frauds across the globe. Managing the risk associated with ATM fraud as well as diminishing its impact is an important issue that faces financial institutions as fraud techniques have become more advanced with increased occurrences.

Diebold (2002) indicated that the ATM is only one of many electronic funds transfer (EFT) devices that are vulnerable to fraud attacks. Card theft, or the theft of card data, is the primary objective for potential thieves because the card contains all relevant account information needed to access an account. Recent global ATM consumer research indicates that one of the most important issues for consumers when using an ATM was personal safety and security. As financial institutions use the migration of cash transactions to self-service terminals as a primary method of increasing branch efficiencies, the ATM experience must be as safe and accommodating as possible for consumers.

The industry has grave difficulty in measuring ATM fraud given the lack of a national classification, the secrecy surrounding such frauds, and the unfortunate fact that one

cannot know the true cost of fraud until one is hit with same. Even low-cost solutions, such as customer awareness, challenge banks that fear scaring customers away from the ATM, or worse, into the doors of a competitor.

Therefore, a face-based ATM security model is presented in this thesis that may address the problem outlined above.

1.3 Research Aims and Objectives

The specifics of this study are to:

(i) develop a face-based ATM security model for financial transactions, that is fast, reasonably simple and accurate in a constrained environment.

(ii) Implement the face-based model in (i).

1.4 Research Methodology

A review of related literature on e-banking, frauds at ATMs, biometrics, biometrics characteristics, biometrics system model, application of biometrics, approaches to face recognition, strong authentication in e-banking, importance of risk assessment, identity management and approaches, and architecture of a face-based ATM security system were presented. A face-based ATM model using principal component analysis (PCA) was developed. A face image Γ_i is transformed into its eigenface components by a simple operation: $w_k = u_k^T (T - \psi)$, where k = 1,2,….M'. The weights obtained as above form a vector $\Omega^T = [w_1, w_2, w_3 ,.... w_{M'}]$ that describes the contribution of each eigenface in representing the input face image. The vector may then be used in a standard pattern

recognition algorithm to find out which of a number of predefined face class, if any, best describes the face. The face class can be calculated by averaging the weight vectors for the images of one individual. The face classes to be made depend on the classification to be made like a face class can be made of all the images where subject has the spectacles. With this face class, classification can be made if the subject has spectacles or not. The Euclidean distance of the weight vector of the new image from the face class weight vector can be calculated as: $\varepsilon_k = || \Omega - \Omega_k||$, where Ω_k is a vector describing the kth face class. The face is classified as belonging to class k when the distance ε_k is below some threshold value $\theta\varepsilon$. Otherwise the face is classified as unknown. Also it can be found whether an image is a face image or not by simply finding the squared distance between the mean adjusted input image and its projection onto the face space: $\varepsilon^2 = || \Phi - \Phi_f ||$, where Φ_f is the face space and $\Phi = T_i - \Psi$ is the mean adjusted input. With this we can classify the image as known face image, unknown face image and not a face image. The system was implemented using MATLAB software on windows operating system platform.

1.5 Expected Contributions To Knowledge

The research work provides a more secured way of identification and authentication using facial recognition which can be applied to ATM banking and even in forensic and other areas where authentication is of utmost paramount.

1.6 Organisation of the Thesis

The rest of the thesis is organised as follows: chapter two presents a review of related literature while chapter three consists of the face-based ATM model. Chapter four presents the implementation of the ATM system while chapter five concludes the thesis with recommendations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

Traditional banks offer many services to their customers, including accepting customer money deposits, providing various banking services to customers, and availability of loans to individuals and companies. Compared with traditional channels of offering banking services through physical branches, e-banking uses the Internet to deliver traditional banking services to their customers, such as opening accounts, transferring funds, and electronic bill payment.

E-banking can be offered in two main ways. First, an existing bank with physical offices can also establish an online site and offer e-banking services to its customers in addition to the regular channel. For example, Citibank is a leader in e-banking, offering walk-in, face-to-face banking at its branches throughout many parts of the world as well as e-banking services through the World Wide Web (Zillman, 2008). Citibank customers can access their bank accounts through the internet, and in addition to the core e-banking services such as account balance inquiry, funds transfer, and electronic bill payment, Citibank also provides premium services including financial calculators, online stock quotes, brokerage services, and insurance.

E-banking from banks like Citibank complements those banks' physical presence. Generally, e-banking is provided without extra cost to customers. Customers are attracted

by the convenience of e-banking through the internet, and in turn, banks can operate more efficiently when customers perform transactions by themselves rather than going to a branch and dealing with a branch representative.

In addition to traditional banks that have both a physical and online presence, there are several e-banks that exist only on the Internet, allowing users to work with a "virtual" bank. NetBank is such an Internet-only bank. Without physical branches, NetBank can cut operating costs and can potentially offer higher deposit rates to its customers and waive many fees normally charged by a bank with a large network of physical branches (*www.encyclopedia.com*). The challenge for Internet-only banks is to provide quality customer services without physical offices. One way in which NetBank is dealing with this issue is via an agreement with the Money Access Centre (MAC ATM) Network, thus providing its customers access to nearly 18,000 ATMs across the United States. NetBank customers can deposit and withdraw funds from their NetBank accounts through these ATMs, and in addition, customers can also deposit and receive funds through wire transfer.

E-banking services are delivered to customers through the Internet and the web using Hypertext Markup Language (HTML). In order to use e-banking services, customers need Internet access and web browser software. Multimedia information in HTML format from online banks can be displayed in web browsers. The heart of the e-banking application is the computer system, which includes web servers, database management

systems, and web application programs that can generate dynamic HTML pages (*java.sun.com*)

Bank customers' account and transaction information is stored in a database, a specialized software that can store and process large amounts of data in high speed. The function of the web server is to interact with online customers and deliver information to users through the Internet. When the web server receives a request such as an account inquiry from an online customer, it requires an external web application program to process the request. C, Visual Basic, VBScript, and Java are some of the languages that can be used to develop web application programs to process customer requests, interact with the database, and generate dynamic responses. Then, the web server will forward the response HTML files to e-banking customers. Several banks, such as NationsBank, also use state-of-the-art imaging systems, allowing customers to view images of cheques and invoices over the Internet (*www.encyclopedia.com).*

One of the main concerns of e-banking is security. Without great confidence in security, customers are unwilling to use a public network, such as the Internet, to view their financial information online and conduct financial transactions. Some of the security threats include invasion of individuals' privacy and theft of confidential information. Banks with e-banking service offer several methods to ensure a high level of security through: (i) identification and authentication, (ii) encryption, and (iii) firewalls. First, the identification of an online bank takes the form of a known Uniform Resource Locator

(URL) or Internet address, while a customer is generally identified by his or her login ID and password to ensure only authenticated customers can access their accounts. Second, messages between customers and online banks are all encrypted so that a hacker cannot view the message even if the message is intercepted over the Internet. The particular encryption standard adopted by most browsers is called Secure Socket Layer (SSL). It is built in the web browser program and users do not have to take any extra steps to set up the program. Third, banks have built firewalls, which are software or hardware barriers between the corporate network and the external Internet, to protect the servers and bank databases from outside intruders. For example, Wells Fargo Bank connected to the Internet only after it had installed a firewall and made sure the firewall was sufficiently impenetrable (netlab.cs.iitm.ernet.in/cs648/2009/assignment1/cs09m034.pdf).

The range of e-banking services is likely to increase in the future. Some banks plan to introduce electronic money and electronic checks. Electronic money can be stored in computers or smart cards and consumers can use the electronic money to purchase small value items over the Internet. Electronic checks will look similar to paper checks, but they can be sent from buyers to sellers over the Internet, electronically endorsed by the seller, and forwarded to the seller's bank for electronic collection from the buyer's bank (*http://www.wncylopedia.com/doc/1G2-3401200518.html*). Further, banks seek to offer their customers more products and services such as insurance, mortgage, financial planning, and brokerage. This will not only deliver more value to the customers but also help banks to grow business and revenues.

2.2 Frauds at ATMs

Diebold (2002), indicated that fraud at the ATM although more difficult than at a Point of Sale (POS), has recently become more widespread. Recent occurrences of ATM fraud range from techniques such as shoulder surfing and card skimming to highly advanced techniques involving software tampering and/or hardware modifications to divert, or trap the dispensed currency.

Recent Global ATM consumer research indicates that one of the most important issues for consumers when using an ATM was personal safety and security. As financial institutions use the migration of cash transactions to self service terminals as a primary method of increasing branch efficiencies, the ATM experience must be as safe and accommodating as possible for consumers.

The Magazine (1991), published that the UK Consumer Association reported a case of phantom withdrawals. In 1989, 570 pounds was wrongly deducted from John Allans' Bank of Scotland account. A total of 8 cash withdrawals were carried out, three of them when he was away with his card in Andorra. Complaining to the bank was fruitless and later Mr. Allan was going to sue the bank of Scotland. The day before the case was due to come to court, the bank reached an out-of court settlement with him. The magazine concludes that this case marks a breakthrough because the bank acknowledged that money can get debited to an account without the use of the card plus the PIN.

This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

Isaca (2007), highlighted that the key to controlling transaction risk lies in adapting effective policies, procedures, and controls to meet the new risk exposures introduced by e-banking. Basic internal controls including segregation of duties, dual controls, and reconcilements remain important. Information security controls, in particular, become more significant requiring additional processes, tools, expertise, and testing. Institutions should determine the appropriate level of security controls based on their assessment of the sensitivity of the information to the customer and to the institution and on the institution's established risk tolerance level.

There are three basic types of ATM attacks: attempts to steal a customer's bank card information; computer and network attacks against ATMs to gather bank card information; and physical attacks against the ATM.

The other most common cash dispenser fraud has become known as the "Lebanese loop" because criminals of Lebanese origin apparently first used it. This has many variations but usually involves the cash machine being tampered with so that your card is not returned to you and is then removed by the criminals: alternatively if you get your card back a device has recorded the details of your magnetic stripe. The crooks have also captured your PIN number though some variation of shoulder surfing. It is this problem

that has led to banks putting posters and other warnings on ATMs advising customers to visually inspect the machine to see if it has been altered or tampered with.

2.3 Biometrics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications. Examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight. The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centres (e.g., credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals.

The overarching task in an identity management system is the determination (or verification) of an individual's identity (or claimed identity). Such an action may be necessary for a variety of reasons but the primary intention, in most applications, is to prevent impostors from accessing protected resources. Traditional methods of establishing a person's identity include knowledge-based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of identity can

easily be lost, shared, manipulated or stolen thereby compromising the intended security. Biometrics offers a natural and reliable solution to certain aspects of identity management, by utilizing fully automated or semi-automated schemes to recognize individuals, based on their biological characteristics. By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.

The effectiveness of an authenticator (biometric or non-biometric) is based on its relevance to a particular application as well as its robustness to various types of malicious attacks. O'Gorman lists a number of attacks that can be launched against authentication systems based on passwords and tokens: (a) client attack (e.g., guessing passwords, stealing tokens); (b) host attack (e.g., accessing plain text file containing passwords); (c) eavesdropping (e.g., "shoulder surfing" for passwords); (d) repudiation (e.g., claiming that token was misplaced); (e) trojan horse attack (e.g., installation of bogus log-in screen to steal passwords); and (f) denial of service (e.g., disabling the system by deliberately supplying an incorrect password several times). While some of these attacks can be deflected by incorporating appropriate defence mechanisms, it is not possible to handle all the problems associated with the use of passwords and tokens.

Biometrics offers certain advantages such as negative recognition and non-repudiation that cannot be provided by tokens and passwords. Negative recognition is the process by

which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it. This is especially critical in applications such as welfare disbursement where an impostor may attempt to claim multiple benefits (i.e., double dipping) under different names. Non-repudiation is a way to guarantee that an individual who accesses a certain facility cannot later deny using it (e.g., a person accesses a certain computer resource and later claims that an impostor must have used it under falsified credentials).

Biometric systems use a variety of physical or behavioural characteristics as shown in Fig. 2.1, including fingerprint, face, hand/finger geometry, iris, retina, signature, gait, palmprint, voice pattern, ear, hand vein, odour or the DNA information of an individual to establish identity. In the biometric literature, these characteristics are referred to as traits, indicators, identifiers or modalities. While biometric systems have their own limitations, they have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides bolstering security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords.

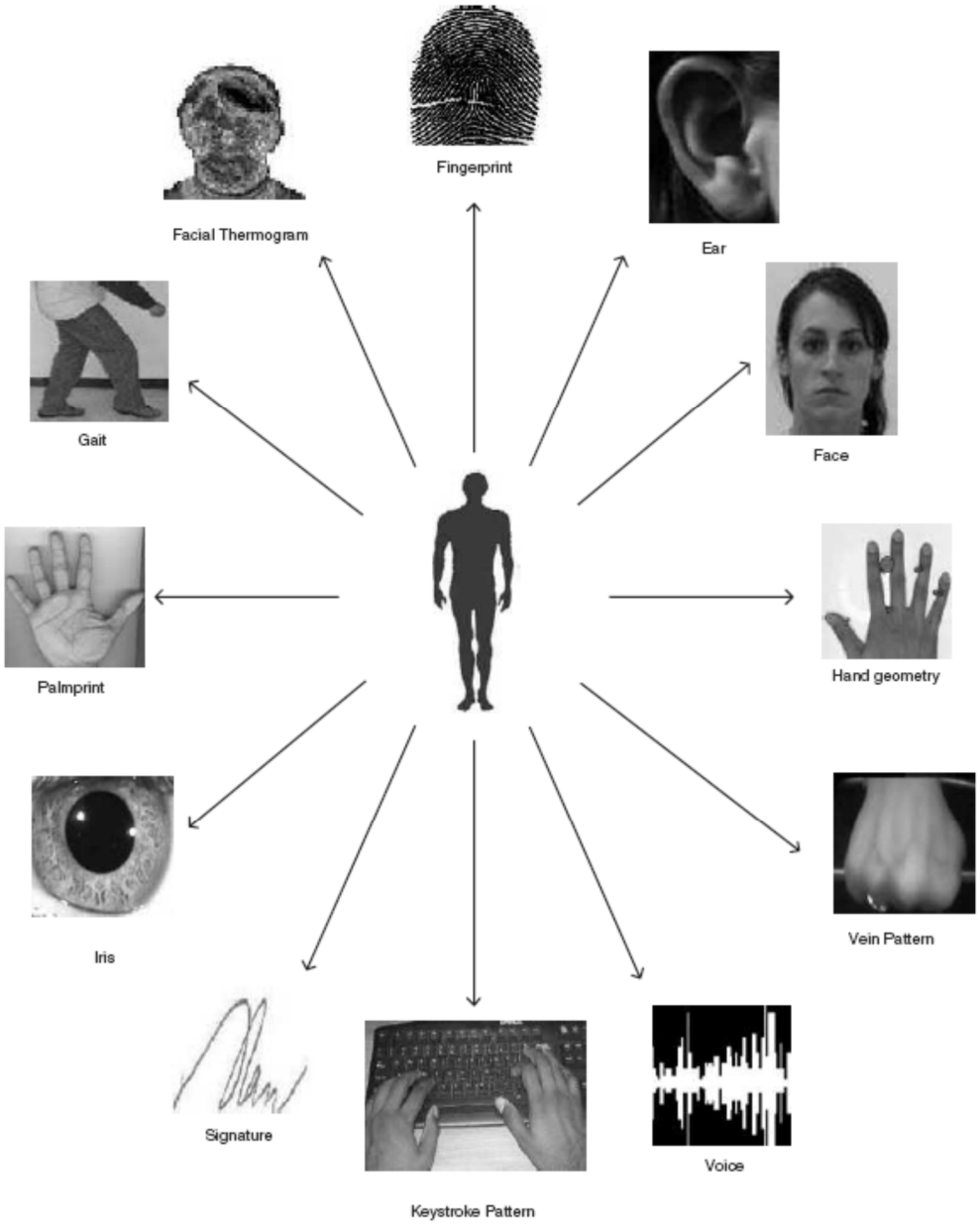


Fig. 2.1 – Biometric traits that can be used for authenticating an individual.

Source**:** Anil K. Jain and Avon Ross and Salil Prahakar (2004).

Physical traits include fingerprint, iris, face and hand geometry while behavioural traits include signature, keystroke dynamics and gait.

No single biometric is expected to effectively meet all the requirements such as accuracy, practicality and cost imposed by all applications (e.g., digital rights management, access control, welfare distribution). In other words, no biometric is ideal but a number of them are admissible. The relevance of a specific biometric to an application is established depending upon the nature and requirements of the application, and the properties of the biometric characteristic. A brief introduction to some of the commonly used biometric characteristics is given in items a to i below:

a. **Face**: Face recognition is a non-intrusive method, and facial attributes are probably the most common biometric features used by humans to recognise one another. The applications of facial recognition range from a static, controlled "mug-shot" authentication to a dynamic, uncontrolled face identification in a cluttered background. The most popular approaches to face recognition are based on either (i) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips, and chin and their spatial relationships, or (ii) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. While the authentication performance of the face recognition systems that are commercially available is reasonable, they impose a number of restrictions on how the facial images are obtained, often requiring a fixed and simple background with controlled illumination. These systems also have difficulty in matching face images captured from two different views, under different illumination conditions, and at different times. It is questionable whether the face itself, without any contextual information, is a sufficient basis for recognizing a

person from a large number of identities with an extremely high level of confidence. In order for a facial recognition system to work well in practice, it should automatically (i) detect whether a face is present in the acquired image; (ii) locate the face if there is one; and (iii) recognize the face from a general viewpoint (i.e., from any pose) under different ambient conditions.

b. **Fingerprint**: Humans have used fingerprints for personal identification for many decades. The matching (i.e., identification) accuracy using fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip whose formation is determined during the first seven months of foetal development. It has been empirically determined that the fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, most fingerprint scanners cost less when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications. The accuracy of the currently available fingerprint recognition systems is adequate for authentication systems in several applications, particularly forensics. Multiple fingerprints of a person provide additional information to allow for large-scale identification involving millions of identities. One problem with large-scale fingerprint recognition systems is that they require a huge amount of computational resources, especially when operating in the identification mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental or occupational reasons

(e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

c. **Hand Geometry**: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and the lengths and widths of the fingers. Commercial hand geometry-based authentication systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to adversely affect the authentication accuracy of hand geometry-based systems. However, the geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Furthermore, hand geometry information may not be invariant during the growth period of children. In addition, an individual's jewellery (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are authentication systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but still much larger than those used for procuring certain other traits (e.g., fingerprint, face, voice).

d. **Palmprint**: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fingerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a lower resolution scanner, which would be cheaper. Finally, when using a high-resolution palmprint scanner, all the features of the hand such as geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

e. **Iris**: The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during foetal development and stabilizes during the first two years of life (the pigmentation, however, continues changing over an extended period of time. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and support the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and even the irises of identical twins are different. It is possible to detect contact lenses printed with a fake iris. The hippus movement of the eye may also be used as a measure of liveness for this biometric. Although early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become

more user-friendly and cost-effective. While iris systems have a very low Far Acceptance Rate (FAR) compared to other biometric traits, the False Rejection Rate (FRR) of these systems can be rather high.

f. **Keystroke**: It is hypothesized that each person types on a keyboard in a characteristic way. This biometric is not expected to be unique to each individual but it may be expected to offer sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioural biometric; one may expect to observe large intra-class variations in a person's typing patterns due to changes in emotional state, position of the user with respect to the keyboard, type of keyboard used, etc. The keystrokes of a person could be monitored unobtrusively as that person is keying in information. This biometric permits "continuous verification" of an individual's identity over a session after the person logs in using a stronger biometric such as fingerprint or iris.

g. **Signature**: The way a person signs her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of authentication. With the proliferation of PDAs and tablet PCs, online signature may emerge as the biometric of choice in these devices. Signature is a behavioural biometric that changes over a period of time and is influenced by the physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their

signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the signature verification system.

h. **Voice**: Voice is a combination of physical and behavioural biometric characteristics. The physical features of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physical characteristics of human speech are invariant for an individual, but the behavioural aspect of the speech changes over time due to age, medical conditions (such as common cold), emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background noise. Speaker recognition is most appropriate in telephone-based applications but the voice signal is typically degraded in quality by the communication channel.

i. **Gait**: Gait refers to the manner in which a person walks, and is one of the few biometric traits that can be used to recognize people at a distance. Therefore, this trait is very appropriate in surveillance scenarios where the identity of an individual can be surreptitiously established. Most gait recognition algorithms

attempt to extract the human silhouette in order to derive the spatio-temporal attributes of a moving individual. Hence, the selection of a good model to represent the human body is pivotal to the efficient functioning of a gait recognition system. Some algorithms use the optic flow associated with a set of dynamically extracted moving points on the human body to describe the gait of an individual. Gait-based systems also offer the possibility of tracking an individual over an extended period of time. However, the gait of an individual is affected by several factors including the choice of footwear, nature of clothing, affliction of the legs and walking surface.

2.3.1 Enrolment, Template, Algorithm, And Verification

In a biometric system, a physical trait needs to be recorded. The recording is referred to as an enrolment. This enrolment is based on the creation of a template. A template is the digital representation of a physical trait. The template is normally a long string of alphanumeric characters that describe, based on a biometric algorithm, characteristics or features of the physical trait. The biometric algorithm can be viewed as the recipe for turning raw ingredients - like a physical trait - into a digital representation in the form of a template. The algorithm will also allow the matching of an enrolled template with a new template just created for verifying an identity, called a *live template*. When a stored template and a live template are compared, the system calculates how closely they match. If the match is close enough, a person will be verified. If the match is not close enough, a person will not be verified.

2.3.2 False Acceptance Rate (FAR), False Rejection Rate (FRR), and Failure to Enrol (FTE)

As described above, when a stored and live template are compared, they either match or not. What happens if it is not you who is trying to match to your template? In this case, someone else is trying to verify as you. If that person were to match as you, it would be classified as a false acceptance. The probability of this happening is referred to as the false acceptance rate, or FAR. The FAR normally states, either in a percentage or a fraction, the probability of someone else matching as you. Thus, the lower the probability, the less likely a match. That means that a match needs to be closer to the original template. As the closeness of a match increases, what does this mean for you when you try to verify as yourself? It means that your live template must match even closer to the enrolled template. If you fail to match against your own template, then you have been falsely rejected. The probability of this happening is referred to as the false rejection rate, or FRR. Thus, the higher the probability of false rejection, the greater the likelihood you will be rejected.

Lastly, when you are new to a biometric system and need to enrol but cannot, this is called a failure to enrol, or FTE. The FTE normally states, either in a percentage or a fraction, the possibility of someone failing to enrol in a system.

2.3.3 A System Model

A biometric system is essentially a pattern recognition system that acquires biometric data from an individual, stores and/or processes data at another location, extracts a salient feature set from the data, compares this feature set against the feature set(s) stored in the database, and executes an action based on the result of the comparison. Therefore, Fig. 2.2 shows a generic biometric authentication system divided into five subsystems: data collection, transmission, signal processing, decision and data storage. We will consider these subsystems one at a time.

2.3.4 Data Collection

Biometric systems begin with the measurement of a behavioural/physiological characteristic. Key to all systems is the underlying assumption that the measured biometric characteristic is both distinctive between individuals and repeatable over time for the same individual. The problems in measuring and controlling these variations begin in the data collection subsystem.

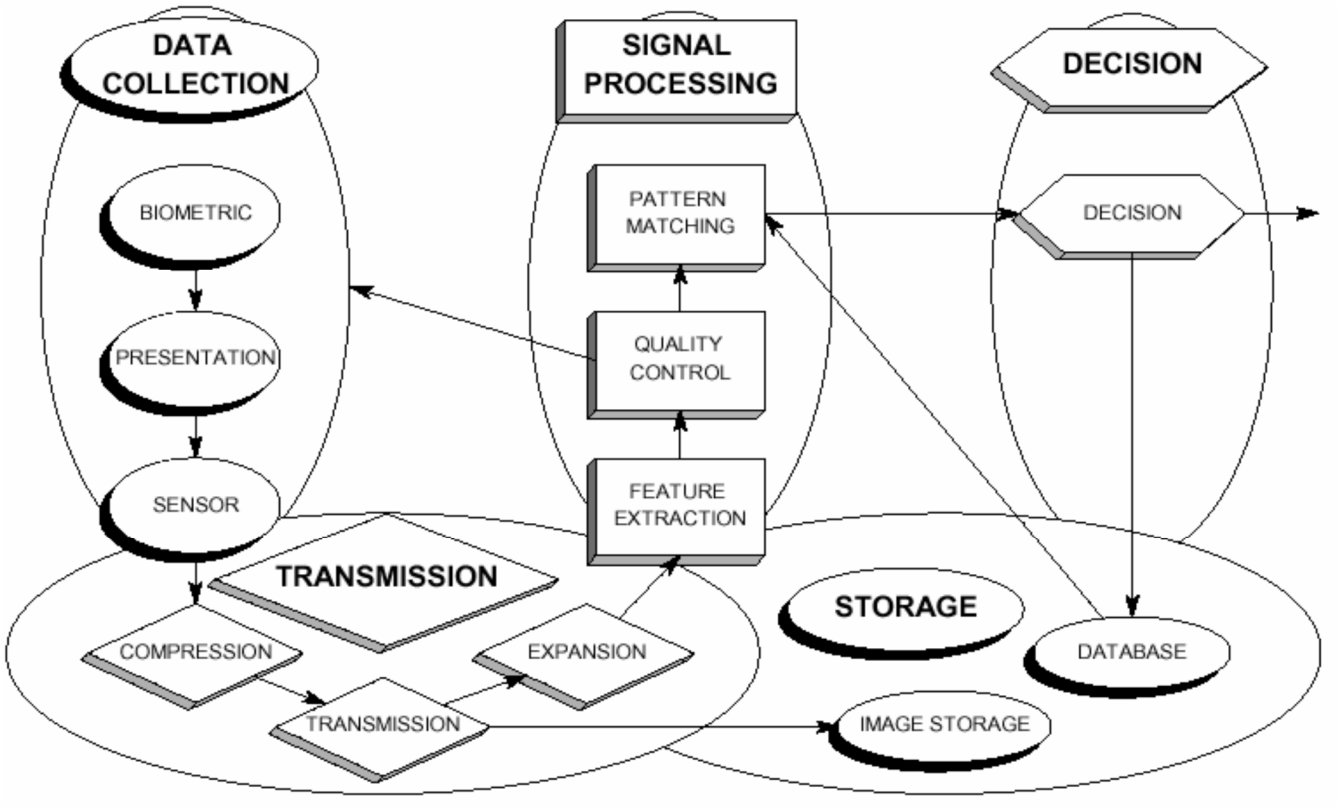


Fig2.2Generic Biometric Authentication System

Source: *National Biometric Test Center Collected Works*" Dr. Wayman Aug 2000.

The user's characteristic must be presented to a sensor. The presentation of any biometric characteristic to the sensor introduces a behavioural (and, consequently, psychological) component to every biometric method. This behavioural component may vary widely between users, between applications, and between the test laboratory and the operational environment. The output of the sensor, which is the input data upon which the system is built, is the convolution of: (1) the biometric measure; (2) the way the measure is presented; and (3) the technical characteristics of the sensor. Both the repeatability and the distinctiveness of the measurement are negatively impacted by changes in any of these factors. If a system is to be open, the presentation and sensor characteristics must be

standardized to ensure that biometric characteristics collected with one system will match those collected on the same individual by another system. If a system is to be used in an overt, non-cooperative application, the user must not be able to wilfully change the biometric or its presentation sufficiently to avoid being matched to previous records.

2.3.5 Transmission

Some, but not all, biometric systems collect data at one location but store and/or process it at another. Such systems require data transmission. If a great amount of data is involved, compression may be required before transmission or storage to conserve bandwidth and storage space. Fig.2.2 shows compression and transmission occurring before the signal processing and image storage. In such cases, the transmitted or stored compressed data must be expanded before further use. The process of compression and expansion generally causes quality loss in the restored signal, with loss increasing with increasing compression ratio. The compression technique used will depend upon the biometric signal. An interesting area of research is in finding, for a given biometric technique, compression methods with minimum impact on the signal-processing subsystem.

If a system is to be open, compression and transmission protocols must be standardized so that every user of the data can reconstruct the original signal. Standards currently exist for the compression of fingerprints (wavelet scalar quantization), facial images (JPEG), and voice data (code excited linear prediction).

2.3.6 Signal Processing

Having acquired and possibly transmitted a biometric characteristic, we must prepare it for matching with other like measures. Fig. 2.2 divides the signal-processing subsystem into four tasks: segmentation, feature extraction, quality control, and pattern matching.

Segmentation is the process of finding the biometric pattern within the transmitted signal. For example, a facial recognition system must first find the boundaries of the face or faces in the transmitted image. A speaker verification system must find the speech activity within a signal that may contain periods of non-speech sounds. Once the raw biometric pattern of interest has been found and extracted from larger signal, the pattern is sent to the feature extraction process.

Feature extraction is fascinating. The raw biometric pattern, even after segmentation from the larger signal, contains non-repeatable distortions caused by the presentation, sensor and transmission processes of the system. These non-controllable distortions and any non-distinctive or redundant elements must be removed from the biometric pattern, while at the same time preserving those qualities that are both distinctive and repeatable. These qualities expressed in mathematical form are called “features”. In a text-independent speaker recognition system, for instance, we may want to find the features, such as the mathematical frequency relationships in the vowels, which depend only upon the speaker and not upon the words being spoken, the health status of the speaker, or the speed, volume and pitch of the speech. There are as many wonderfully creative mathematical

approaches to feature extraction as there are scientists and engineers in the biometrics industry.

In general, feature extraction is a form of non-reversible compression, meaning that the original biometric image cannot be reconstructed from the extracted features. In some systems, transmission occurs after feature extraction to reduce the requirement for bandwidth.

After feature extraction, or maybe even before, we will want to check to see if the signal received from the data collection subsystem is of good quality. If the features "don't make sense" or are insufficient in someway, we can conclude quickly that the received signal was defective and request a new sample from the data collection subsystem while the user is still at the sensor. The development of this "quality control" process has greatly improved the performance of biometric systems in the last few short years. On the other hand, some people seem never to be able to present an acceptable signal to the system. If a negative decision by the quality control module cannot be overridden, a "failure to enrol" error results.

The feature "sample", now of very small size compared to the original signal, will be sent to the pattern matching process for comparison with one or more previously identified and stored feature templates or models. We use the term "template" to indicate stored features. The features in the template are of the same type as those of a sample. For instance, if the sample features are a "vector" in the mathematical sense, then the stored

template will also be a “vector”. The term “model” is used to indicate the construction of a more complex mathematical representation capable of generating features characteristic of a particular user. Models and features will be of different mathematical types and structures. Models are used in some speaker and facial recognition systems. Templates are used in fingerprint, iris, and hand geometry recognition systems.

The term “enrolment” refers to the placing of a template or model into the database for the very first time. Once in the database and associated with an identity by external information (provided by the enrolee or others), the enrolment biometric data is referred to as the template or model for the individual to which it refers.

The purpose of the pattern matching process is to compare a presented feature sample to the stored data, and to send to the decision subsystem a quantitative measure of the comparison. An exception is enrolment in systems allowing multiple enrolments. In this application, the pattern matching process can be skipped. In the cooperative case where the user has claimed an identity or where there is but a single record in the current database (which might be a magnetic stripe card), the pattern matching process might only make a comparison against a single stored template. In all other cases, such as large-scale identification, the pattern matching process compares the present sample to multiple templates or models from the database one at a time, as instructed by the decision subsystem, sending on a quantitative “distance” measure for each comparison. In place of a “distance” measure, some systems use “similarity” measures, such as maximum likelihood values.

The signal processing subsystem is designed with the goal of yielding small distances between enrolled models/templates and later samples from the same individual and large distances between enrolled models/templates and samples of different individuals. Even for models and samples from the same individual, however, distances will rarely, if ever, be zero, as there will always be some non-repeatable biometric-, presentation-, sensor- or transmission-related variation remaining after processing.

2.3.7 Storage

The remaining subsystem to be considered is that of storage. There will be one or more forms of storage used, depending upon the biometric system. Templates or models from enrolled users will be stored in a database for comparison by the pattern matcher to incoming feature samples. For systems only performing "one-to-one" matching, the database may be distributed on smart cards, optically read cards or magnetic stripe cards carried by each enrolled user. Depending upon system policy, no central database need exist, although in this application a centralized database can be used to detect counterfeit cards or to reissue lost cards without re-collecting the biometric pattern.

The database will be centralized if the system performs one-to-*N* matching with *N* greater than one, as in the case of identification or "PIN-less verification" systems. As *N* gets very large, system speed requirements dictate that the database be partitioned into smaller subsets such that any feature sample need only be matched to the templates or models stored in one partition, or indexed by using an appropriate data structure which allows the

templates to be visited in an advantageous order during the retrieval. These strategies have the effect of increasing system speed and decreasing false matches, at the expense of increasing the false non-match rate owing to partitioning errors. This means that system error rates do not remain constant with increasing database size and identification systems do not scale linearly. Consequently, database partitioning/indexing strategies represent a complex policy decision.

If it may be necessary to reconstruct the biometric patterns from stored data, raw (although possibly compressed) data storage will be required. The biometric pattern is generally not reconstructable from the stored templates or models, although some methods do allow a coarse reconstruction of patterns from templates. Further, the templates themselves are created using the proprietary feature extraction algorithms of the system vendor. The storage of raw data allows changes in the system or system vendor to be made without the need to re-collect data from all enrolled users.

2.3.8 Decision

The decision subsystem implements system policy by directing the database search, determines “matches” or “non-matches” based on the distance or similarity measures received from the pattern matcher, and ultimately makes an “accept/reject” decision based on the system policy. Such a decision policy could be to reject the identity claim (either positive or negative) of any user whose pattern could not be acquired. For an acquired pattern, the policy might declare a match for any distance lower than a fixed threshold and “accept” a user identity claim on the basis of this single match, or the

policy could be to declare a match for any distance lower than a user-dependent, time-variant, or environmentally linked threshold and require matches from multiple measures for an "accept" decision. The policy could be to give all users, good guys and bad guys alike, three tries to return a low distance measure and be "accepted" as matching a claimed template. Or, in the absence of a claimed template, the system policy could be to direct the search of all, or only a portion, of the database and return a single match or multiple "candidate" matches. The decision policy employed is a management decision that is specific to the operational and security requirements of the system. In general, lowering the number of false non-matches can be traded against raising the number of false matches. The optimal system policy in this regard depends both upon the statistical characteristics of the comparison distances coming from the pattern matcher, the relative penalties for false match and false non-match within the system, and the *a priori* (guessed in advance) probabilities that a user is, in fact, an impostor. In any case, in the testing of biometric devices, it is necessary to decouple the performance of the signal processing subsystem from the policies implemented by the decision subsystem.

2.3.9 Applications Of Biometrics

Establishing the identity of a person with high confidence is becoming critical in a number of applications in our vastly interconnected society. Questions like "Is she really who she claims to be?" "Is this person authorized to use this facility?" or "Is he in the watch list posted by the government?" are routinely being posed in a variety of scenarios ranging from issuing a driver's licence to gaining entry into a country. The need for

reliable user authentication techniques has increased in the wake of heightened concerns about security, and rapid advancements in networking, communication and mobility. Thus, biometrics is being increasingly incorporated in several different applications. These applications can be categorised into two main groups:

a. Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM or credit card use, physical access control, mobile phone, PDA, medical records management, and distance learning.

b. Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare-disbursement, border control and passport control. Forensic applications such as corpse identification, criminal investigation and parenthood determination.

Examples of a few applications where biometrics is being used for authenticating individuals are presented in Fig. 2.3.



Fig. 2.3 Biometric system being deployed in various applications

Source:

a. The *Schiphop Privium program at the Amsterdam airport uses iris scans to validate the identity of a traveller (www.scribd.com).*
b. *A few Kroger store in Texas use fingerprint verification systems that enable customers to render payment at the check-out counter (http://www-staff.it.uts.edu.au-ruodu/Biometriclectures/handbook of biometrics. pdf)*
c. *Contactless palm-vein system have been in some ATMs in Japan(www.fujitsu.com*/downloads/GLOBAL/labs/papers/palmvein.pdf *)*
d. *http://biometrics.cse.msu.edu/publications/thesis/karthiknardakumar_biometricsfusionMSO5.PDF*
e. *http://biometrics.cse.msu.edu/publications/thesis/karthiknardakumar_biometricsfusionMSO5.PDF*

2.3.10 Biometric Characteristics

A number of biometric characteristics are being used in various applications. Each biometric has its pros and cons and, therefore, the choice of a biometric trait for a particular application depends on a variety of issues besides its matching performance. Seven factors that determine the suitability of a physical or a behavioural trait to be used in a biometric application have been identified as follows:

Universality: Every individual accessing the application should possess the trait.

Uniqueness: The given trait should be sufficiently different across individuals comprising the population.

Permanence: The biometric trait of an individual should be sufficiently invariant over a period of time with respect to the matching algorithm. A trait that changes significantly over time is not a useful biometric.

Measurability: It should be possible to acquire and digitize the biometric trait using suitable devices that do not cause undue inconvenience to the individual. Furthermore, the acquired raw data should be amenable to processing in order to extract representative feature sets.

Performance: The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.

Acceptability: Individuals in the target population that will utilize the application should be willing to present their biometric trait to the system.

Circumvention: This refers to the ease with which the trait of an individual can be imitated using artefact e.g., fake fingers (in the case of physical traits), and mimicry (in the case of behavioural traits).

2.4 Strong Authentication in E-banking

2.4.1 The Importance of a Two-Factor Authentication in E-banking

In today's corporate environment, the need arises to ensure that only authorised individuals or customers gain access to critical devices or services offered. With the availability of ready to use "sniffers" and access code (password/PIN) cracking tools, the standard username/password or PIN combination may no longer be adequate to withstand the test of secure authentication.

Other means of discovering password(s) or PIN(s) are aided by bad habits. Many customers and users in general use easy-to-guess combinations, make infrequent changes, and often write their password or PIN down and leave it in conspicuous places, for example stuck to the computer monitor. Some customers not only never change their password or PIN, but also assign the same value to all their online access codes and even to their ATM cards.

Many organisations are depending on sophisticated and complex networks, which have become one of the most important channels to do business through. It is becoming an accepted fact that using a single factor authentication method may not be adequate to serve the growing high-risk e-business market place from a security point of view.

Authentication, however, cannot exist in a vacuum; it must be part of a security framework. The four security control objectives that address an adequate security framework are: (i) identification and authentication - to prove identity and allow access to assets; (ii) integrity - ensure that data was changed by the authorised person and that no unauthorised changes have been made; (iii) confidentiality - restricting data access to the people authorised to see it; and (iv) non-repudiation - one may not deny his/her actions.

This section gives an insight into strong user authentication in relation to electronic B2B (business-to-business) and B2C (business-to-customer).

2.4.2 What Is Strong User Authentication?

Reliable customer authentication is imperative for financial institutions engaging in any form of electronic banking or commerce. An effective authentication system can help financial institutions reduce fraud and strengthen the security framework that underlies the application. Strong customer authentication practices are also necessary to enforce anti-money laundering measures and help financial institutions detect and reduce identity thefts.

Customer interaction with financial institutions is migrating from physical recognition and paper–based documentation to remote electronic access and transaction initiation. The risks of doing business with unauthorised or incorrectly identified individuals in an electronic banking environment could result in financial loss and reputation damage

through fraud, disclosure of confidential information, corruption of data and agreements that the organisation may not be able to enforce.

2.4.3 Two-factor Authentication And Non-repudiation

Accountability (non-repudiation) is a key concern for organisations. It is important – and in many cases critical – to ensure that employees and customers are accountable for the electronic transactions they perform.

Token and smart cards, for example, help ensure this accountability because each employee or customer is expected to be in physical possession of his/her own token/smart card, and each should be the only person to know the PIN for accessing the services on that device. This is to a great extent a policy issue, but such devices help enforce that policy. Because the device is unique to the employee or customer. Any transactions - such as system logon, transactions made on the system - performed with that device are reasonably certain to have been performed by the person to whom that device was issued because the device is unique to the employee or customer, Such devices make it very hard, if not impossible, for employees or customers to successfully repudiate the transactions they have executed.

For a user to be able to access a resource, it must be determined if this individual is who he claims to be, if he has the necessary credentials, and if he has been given the necessary rights/privileges to perform the actions he is requesting. Identification and authentication describes a method of ensuring that the user is in fact who he claims to be. Once these

steps are completed successfully, the user can access and use the system resources. However, it is necessary to track the user's activities and enforce accountability for his/her actions - detective controls through audit trail.

Choosing the appropriate identification and authentication tools depends on the channels through which an organisation wishes to provide its services, the flexibility that it wishes to provide its users and customers alike, and the perceived risks.

Specifically, there are three user authentication methods: (i) something you have - this can include a key to a door or a token card; (ii) something you know - passwords or PINs may be classed in this category; and (iii) something you are - this area includes biometric authentication such as fingerprints, voice recognition, retina or iris scans (Available in en.wikipedia.org/wiki/multifactor_ authentication).

Individually, any of the three concepts have problems. "Something you have" may be stolen. "Something you know" may be guessed, shared or lost. "Something you are" is the strongest, but generally the most costly, and may not always be appropriate for integration with some user applications.

Since these single-factor authentication problems exist, the next step is two-factor authentication. For example, ATMs use a combination of a plastic card (something you have) and a four-digit PIN number (something you know).

Requiring two factors significantly enhances security because one factor authentication by itself may not be sufficient to perform authentication that can be relied on. Furthermore, two-factor authentication ensures that any transactions carried out by the user cannot be denied and that the user can be held accountable for his actions on the system, be it an employee in the organisation or a customer of that organisation.

Authentication methods that depend on more than one factor typically are more difficult to compromise than single-factor authentication systems. Accordingly, properly designed and implemented multi-factor authentication methods are more reliable indicators of authentication and stronger fraud deterrents. For example, the use of a logon ID/password is single-factor authentication (something the user knows); whereas, a transaction using an ATM typically requires two-factor authentication: something the user possesses (the card) combined with something the user knows (PIN).

In general, multi-factor authentication methods should be used on higher risks systems, for example remote access to networks or offering a service through the internet e.g. e-banking. A number of financial institutions have been offering their e-banking services dependent only on a PIN, however, many financial institutions are upgrading their systems to include two-factor authentication when offering their services through electronic means.

An effective authentication method should have customer acceptance, ease of use, reliable performance, scalability to accommodate growth, and interoperability with existing systems and strategic plans of the organisation.

No matter what type of two-factor authentication model is used, the organisation should be sensitive to the fact that proper implementation is key to the reliability and security of the system. For example, a poorly implemented two-factor system may be less secure than a properly implemented single-factor system because of weak organisational policy, procedures or standards. This is so, because the human element is the weakest link in any security application or system.

The success of a particular authentication method depends on more than the technology. It also depends on appropriate policies, procedures and controls. On this, organisations may now adopt MSA ISO/IEC 17799:2001 – Information

Technology - Code of Practice for information security management,

MSA-Management System Accreditation, ISO – International Organization for Standardization, IEC – International Electrotechnical Commission. Executive management should give their full support to ensure proper implementation and adherence to policy.

2.4.4 Why Is Strong Authentication Needed In E-banking?

Single-factor authentication usually consists of "something you know". However, generally, these could be susceptible to attacks that could compromise the security of the application. Some of the more common attacks can occur at little or no cost to the perpetrator and without detection.

Such programmes are readily available over the Internet. If undetected, the perpetrator could access the information without alerting the legitimate user. This is the reason for using a strong user authentication process to protect the data and systems. The need for strong user authentication has many benefits.

One example of strong user authentication is amply demonstrated by the use of ATMs – access to an ATM is protected by a strong user authentication; a bankcard, and a PIN. How many customers would use an ATM if only a reusable password or PIN scheme allowed access to their accounts? The same security approach should be applied to electronic banking services, especially when using the Internet, since the perceived risks are by far greater.

In addition to reducing the risk of unauthorised access, two-factor authentication also provides institutions with a foundation to enforce electronic transactions and agreements. First, effective authentication provides the basis for validation of parties to the transaction and their agreement to its terms. Second, it is a necessary element to establish authenticity of the records evidencing the electronic transaction should there ever be a dispute. Third, it is a necessary element to establish the integrity of the records evidencing the electronic transaction. All of these elements promote the enforceability of electronic agreements.

Financial institutions should assess the adequacy of existing authentication techniques in the light of changing or new perceived risks (increasing ability of hackers to compromise

less robust single factor techniques). According to the International Computer Security Association (ICSA), 80 per cent of system undermining occurs from within the organisation (*http://www.speedyadverts.com/SATopics/html/information_security2.html*). The Basle Committee on Banking Supervision advises financial institutions to consider the apparent risks of offering Internet banking services based on PIN alone. Single factor authentication alone may not be commercially reasonable or adequate for high-risk applications and transactions.

Systems linked to open and untrusted networks like the Internet are subject to a greater number of individuals who may attempt to compromise the system. Attackers may use automated programs to systematically generate millions of numerical combinations, in the case of systems relying on PIN alone, to learn a customer's access code (brute force attack).

Would consumers perceive this as a secure way of doing their banking over the internet, which is technically an insecure medium, when at the same time they are obliged to do their banking via an ATM using two-factor authentication?

Consumers rely on, and gain comfort from, a strong user authentication method to protect their sensitive data and money. Also, financial institutions can hold users accountable for controlling their cards and PIN. The combination of two authentication factors is what enables users and financial institutions to hold each other accountable.

2.4.5 The Importance of Risk Assessment

There are a variety of authentication tools and methodologies financial institutions can use to authenticate customers. These include the use of passwords and personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices such as smart cards or other types of "tokens", database comparisons, and biometric identifiers. How whichever authentication tool is chosen heavily depends on the type of service and across which channel together with a risk assessment that the financial institution must carry out in order to ensure that the perceived risks are adequately mitigated.

An effective authentication program should be implemented on an enterprise-wide basis and across all services channels, for example Internet, telephone and call-centre services, to ensure that controls and authentication tools are adequate. Authentication processes should be designed to maximise interoperability and should be consistent with the financial institution's overall strategy for electronic banking and e-commerce customer services.

The implementation of appropriate authentication methodology starts with an assessment of the perceived risks to the institution's electronic banking systems. The perceived risks should be evaluated in the light of the: (i) channel through which the organisation shall be offering its service, for example Internet; (ii) services offered (third-

party bill payment); (iii) monetary-value and frequency of transactions passed through the channel; (iv) sensitivity and value of the stored information to both the institution and the customer; (v) ease of using the method e.g. token card, smart card or PKI (public key infrastructure); and (vi) legislation, that is Banking Act 1994, Prevention of Money Laundering Act 1994, Professional Secrecy Act 1994, Electronic Commerce Act 2001 and the Data Protection Act 2001 (*www.coe.int*).

The use of token or smart card devices in the organisation will cause some major changes - change doesn't come easy. Employees and customers will need to get accustomed to having their cards in their possession at all times. People in general tend to be already accustomed to this fact - hardly anyone ever leaves home without first making sure that the mobile phone is on hand, together with an array of plastic money.

The token card will become just another of those essentials. Most organisations have deployed electronic cards to allow authorised personnel to access their office buildings (*www.speedyadverts.com*). Patrons are no longer given a key to their hotel room but an electronic key card. So really, the culture and acceptance of using token card/smart card based solutions to access electronic banking systems is generally on the upswing.

Token Cards: the most cost-effective solution in e-banking. When it comes to providing e-banking services through different channels using a flexible, portable two-factor authentication model, one of the most cost-effective solutions available are token cards.

A financial institution could opt for a token card-based solution to minimise risk and maintain customer confidence, without the need to invest in software or hardware on the customer's part.

Each customer is given a credit card-sized device with a numeric keypad that is used to safely "unlock" an account information. To access accounts, users must possess both the token card and a PIN to unlock the token card itself - one factor without the other is useless.

Before the server allows logical access to the information, the customer must key in the string of numbers (six generally) that the token card will generate on a one-time-basis. It will have a specific length of valid time, ranging from forty to fifty seconds, during which the customer will have ample time to key it in on either the keyboard or telephone keypad.

The token card's inbuilt security mechanism is in sync with the back-end server, with which the authorisation code generated by the token card will be verified. Each token has a unique serial number that forms part of the cryptographic key for the use of generating dynamic network access codes that change every time the customer needs to log on to the application.

This provides a high level of security because, first of all, with today's computers, it may be possible to "sniff" the cryptographic key and try to break the algorithm that generates the next password using "brute force" techniques that use all the possible combinations.

To prevent eavesdroppers listening or manipulating network traffic, the network path is now also protected by the implementation of a secure channel, for example SSL (www.speedyadverts.com/.../html/information_security3.html - Cached).

In order for the transaction to be authorised and validated, the server generates what is called a "challenge" – a numeric value made up of six characters that is the result of a hashing function using the date, time and value of the transaction itself (www.comarch.com/files.../Comarch_Mobile_Security_EN_479.pdf).

The challenge is presented to the user who in turn keys in this value on the token card that produces the "challenge response", also made up of six characters. This response is valid for that transaction only, and even if it were to become known to third parties eavesdropping on the line, it would be useless for other transactions. Furthermore, if it is manipulated during transmission, the server will reject it, since the server computes its own mathematical calculations to confirm the integrity of the value transmitted.

If the PIN is entered incorrectly for, say, three times (clipping level), the token card will be locked (similar to what happens on an ATM, with the difference that the ATM retains the card). The administrator is the only authorised person who may unlock a blocked card. If the authorisation code is entered incorrectly, the application is generally set to

end the session. All such login attempts are logged (audit trail) and reviewed by the administrator, so that any such unauthorised attempts are immediately identified and dealt with accordingly.

2.4.6 Positive Return on Investment (ROI)

Common sense tells us that the more applications the token card concept may be applied to, the greater the ROI. Nevertheless, every implementation is different, and organisations should perform a thorough cost benefit analysis before proceeding with the implementation of such a token card-based solution. Organisations may adopt token cards for both back-office employees and customers alike.

It is believed that token card deployment that forms an integral part of the backbone of logical access control to sensitive systems will discourage fraudulent transactions by employees and also reduce the need to employ more personnel to supervise back-office transactions.

However, it must be remembered that the human element is the weakest link in any security setup, so adequate segregation of duties is one of those controls that safeguard against abuse. Furthermore, the implementation should be based on a sound information security policy on logical access controls, Thiagarajan (2002) and procedures that management must ensure that they are being adhered to.

2.5 Identity Management

Identity management in an enterprise is a combination of processes and technologies to manage and secure access to the information and resources of an organisation while also protecting user profiles, including customer profiles. It includes the entire process of deciding who should have access to resources, and to what resources; providing, changing and terminating such access when appropriate; managing the process and monitoring it for compliance with internal and external policies. This usually applies to situations where a person has to identify who he/she claims to be by means of a verified identity, such as a passport or identity card at border control, login credentials for e-banking and biometric identification for account access at an ATM machine.

Identity management has two principal components: management "of" the identity and management "by" the identity (Wood, 2005). Management of the identity is the process of issuing and using digital identities and credentials (such as usernames and passwords) for authentication. Management by the identity combines the proven identity of the user with their authorisation, in order to grant access to resources.

2.5.1 Identity Management Models

Identity of an entity has its own life cycle. For example, an employee's login account for accessing the company network would be created, maintained, synchronised and deleted across multiple systems or platforms. The employee's login credentials, with proper access rights, would be granted by a process called user provisioning. This account would be maintained and updated whenever new privileges are assigned to this employee,

perhaps due to internal transfer, promotion or demotion. The employee's data or passwords would be synchronised among different IT systems and platforms. Finally, his/her login credentials can be deleted across all systems due to, say termination of employment or retirement. This removal of access rights is a process called user de-provisioning. There are three common identity management models Jøsang and Pope (2005).

2.5.2 Isolated Identity Management

This model requires that each user possess an identifier for access to each isolated service. This system is used a lot in online services and resources, because it is relatively simple for service providers to manage, but it is rapidly becoming unmanageable for users. The exponential growth in online services has led to users being overloaded with identifiers and credentials (different logins and passwords) that they need to remember and manage. For this reason, new identity management models such as Federated Identity management and Centralised Identity Management are being proposed and implemented.

2.5.3 Federated Identity Management

Federated identity management simplifies the account management problem. A set of agreements and standards are defined among a group of service providers who recognise user identifiers from one another. A customer of one particular service provider could access all services provided by another service provider in the group with only a single identifier. For such standardised methods of information exchange within the group to work, implementation of a common technology standard such as Organisation for the

Advancement of Structured Information Standards (OASIS), Security Assertion Markup Language (SAML), the open source initiative and Shibboleth Project (2004).

2.5.4 Centralised identity management

In this model, the same identifier and credential are used by each service provider. This could for example be implemented by having a PKI, where a Certificate Authority (CA) issues certificates to users. Each user can then use the same certificate to access different services, and all providers authenticate the client through the same certificate before granting access to their services. Another example could be the Single sign-on (SSO) model, which requires a user to login once and be authenticated automatically by all other service providers. The Kerberos Authentication Server and Microsoft .Net Passport are examples of SSO implementation. A drawback of this approach is that should one of the trusted identity providers fail (e.g. under a DoS attack), the normal services of all service providers may be affected.

2.5.5 Authentication and Authorisation

Authentication techniques make use of one or more of the following factors: (i) something you know (e.g. password); (ii) something you have (e.g. a smart card); and (iii) something you are (e.g. fingerprint, your face, your voice) (*Authentication Methods and Techniques* by Christopher Mallow).

If two of these factors are needed for successful authentication, it is termed a "two-factor authentication". Two-factor authentication is generally believed to be more secure, and

therefore many high-risk systems such as Internet banking are now implementing schemes like this.

Authorisation is a process that determines whether an entity is allowed access to a given asset or resource, Barkley, (1995). Common access control models are: (i) discretionary access control (DAC): in this mechanism, users own the objects under their control, and the granting and revoking of access control privileges are left to the discretion of individual users. (ii) mandatory access control (MAC): it is a means of restricting access to objects based on the sensitivity of the information contained in the objects, along with formal authorisation of subjects to access information of such sensitivity; and (iii) role-based access control (RBAC): it is an authorisation mechanism in which access decisions are based on the roles that individual users have as part of an organisation.

When assigning access rights to an entity, the principles of least privilege and separation of duties are strongly recommended. The principle of least privilege recommends that the least amount of privileges necessary to perform one's task should be granted to an entity. The principle of segregation of duties suggests that critical functions are divided into steps among different individuals to prevent a single individual from subverting a critical process.

2.6 APPROACHES TO FACE RECOGNITION

Face recognition has been an active research area over last 30 years. This research spans several disciplines such as image processing, pattern recognition, computer vision, and

neural networks. It has been studied by scientists from different areas of psychophysical sciences and those from different areas of computer sciences. Psychologists and neuroscientists mainly deal with the human perception part of the topic, whereas engineers studying on machine recognition of human faces deal with the computational aspects of face recognition. Face recognition has applications mainly in the fields of biometrics, access control, law enforcement and, security and surveillance systems.

The problem of face recognition can be stated as follows: Given still images or video of a scene, identifying one or more persons in the scene by using a stored database of faces (Chellappa et al, 1995). The problem is mainly a classification problem. Training the face recognition system with images from the known individuals and classifying the newly coming test images into one of the classes is the main aspect of the face recognition systems.

This problem seems to be easily solved by humans where limited memory can be the main problem; whereas the problems for a machine face recognition system are: (i) facial expression change; (ii) illumination change; (iii) aging; (iv) pose change; (v) scaling factor (i.e. size of the image); (vi) frontal versus profile; (vii) presence and absence of spectacles, beard, moustache etc.; and (viii) occlusion due to scarf, mask or obstacles in front. (Jaiswal, Bhadauria, Jadon, 2011).

The problem of automatic face recognition (AFR) is a composite task that involves detection of faces from a cluttered background, facial feature extraction, and face

identification. A complete face recognition system has to solve all sub-problems, where each one is a separate research problem. This research work concentrates on the problem of facial feature extraction and face identification.

Most of the current face recognition algorithms can be categorized into two classes, image template based and geometry feature-based. The template based methods Robert (1981), compute the correlation between a face and one or more model templates to estimate the face identity. Brunelli and Poggio (1993), suggest that the optimal strategy for face recognition is holistic and corresponds to template matching. In their study, they compared a geometric feature based technique with a template matching based system and reported an accuracy of 90% for the first one and 100% for the second one on a database of 97 persons. Statistical tools such as Support Vector Machines (SVM) Osuna *et al.* (1997) and Vladimir (1995), Principal Component Analysis (PCA) (Sirovich and Kirby, 1987) and; Turk and Pentland, (1991), Linear Discriminant Analysis (LDA) Belhumeur *et al.* (1997), kernel methods Scholkopf *et al.* (1998) and Yang (2002), and neural networks Howell *et al.* (1995), Lawrence *et al.* (1998) and; Poggio and Sung (1994), have been used to construct a suitable set of face templates. Other than statistical analysis and neural network approach there are other approaches known as hybrid approaches which use both statistical pattern recognition techniques and neural network systems. Examples for hybrid approaches include the combination of (Principal Component Analysis) PCA and Radial Basis Function (RBF) neural network Er, *et al.* (1999) and Thomas *et al.* (1998). Among other methods, people have used range

Chellappa *et al.* (1995), infrared scanned, Yoshitomi *et al.* (1997) and profile Liposcak *et al.* (1999), images for face recognition. While templates can be viewed as features, they mostly capture global features of the face image. Facial occlusion is often difficult to handle in these approaches.

The geometry feature based methods analyze explicit local facial features, and their geometric relationships. Cootes *et al.* (1997) have presented an active shape model in extending the approach by Yuille (1991). Wiskott *et al.* (1997) developed an elastic bunch graph matching algorithm for face recognition. Penev *et al.* (1996) developed PCA into Local Feature Analysis (LFA). This technique is the basis for one of the most successful commercial face recognition systems, FaceIt. The summary of approaches to face recognition is shown in Fig. 2.4.

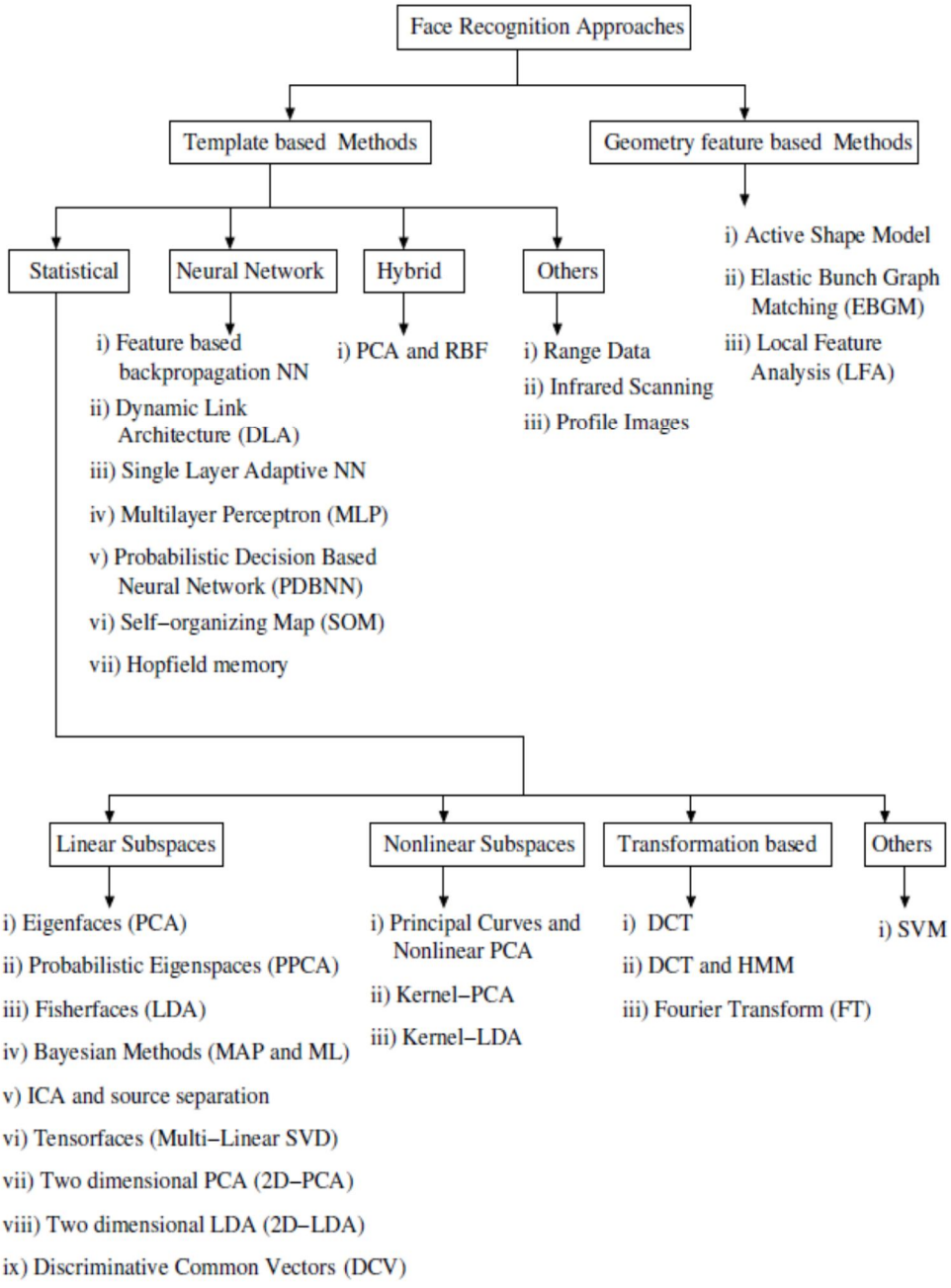


Figure 2.4: Summary of approaches to face recognition.

2.6.1 Template Based Methods

Template matching is conceptually related to holistic approach which attempts to identify faces using global representations Huang (1998). These methods approach the face image

as a whole and try to extract features from the whole face region and then classify the image by applying a pattern classifier. One of the methods used to extract features in a holistic system, is based on statistical approaches which is discussed in section 2.6.2.

2.6.2 Statistical Approaches

Images of faces, represented as high-dimensional pixel arrays, often belong to a manifold of intrinsically low dimension. Face recognition research has witnessed a growing interest in techniques that capitalize on this observation, and apply algebraic and statistical tools for extraction and analysis of the underlying manifold. The techniques that identify, parameterize and analyze linear subspaces are described below. Other than linear subspaces there are some statistical face recognition techniques which are based on nonlinear subspaces (like kernel-PCA and kernel-LDA), transformation (like Discrete Cosine transform (DCT) and HMM and Fourier Transform) and Support Vector Machine (SVM).

Appearance-based approaches for face recognition like PCA, LDA, and probabilistic subspace view a 2D face image as a vector in image space. A set of face images $\{x_i\}$ can be represented as a M x N matrix $X = [x_1, x_2, x_i, \ldots, x_N]$, where M is total number of pixels in the images and N is the total number of samples. Each of the face images x_i belongs to one of the C classes {1, 2, ... , C}.

2.6.3 Neural Network Based Approaches

Artificial Neural Network (ANN) Yegnanarayana (1999), Haykin (1999), Bishop (1995) and Mammone (1993), is a powerful tool for pattern recognition problems. The use of

neural networks (NN) in faces has addressed several problems: gender classification, face recognition and classification of facial expressions. One of the earliest demonstrations of NN for face recall applications is reported in Kohonen's associative map Kohonen (1988). Using a small set of face images, accurate recall was reported even when input image is very noisy or when portions of the images are missing. A few NN based face recognition techniques are discussed in the following.

Single Layer adaptive NN: A single layer adaptive NN (one for each person) for face recognition, expression analysis and face verification was reported in Stonham (1984). A system named Wilke, Aleksander and Stonham's recognition devise (WISARD) was devised. It needs typically 200-400 presentations for training each classifier where the training patterns included translation and variation in facial expressions. One classifier was constructed corresponding to one subject in the database. Classification was achieved by determining the classifier that was giving the highest response for the given input image.

Multilayer Perceptron (MLP): Much of the present literature on face recognition with neural networks present results with only a small number of classes (often below 20). In Demers et al, (1993) the first 50 principal components of the images were extracted and reduced to five dimensions using autoassociative neural network. The resulting representation was classified using a standard multilayer perceptron (MLP).

Self-Organizing map (SOM): Lawrence et al. (1997) presented a hybrid neural network solution which combines local image sampling, a self-organizing map (SOM) and a convolutional neural network. The SOM provides a quantization of the image samples into a topological space are also nearby in the output space, thereby providing dimensionality reduction and invariance to minor changes in the image sample. The convolutional neural network provides partial invariance to translation, rotation, scale and deformation. The recognizer provides a measure of confidence in its output. The classification error approaches zero when rejecting as few as 10% of the examples on a database of 400 images which contains a high degree of variability in expression, pose and facial details.

Hopfield memory model: Hopfield memory model for the facial images is organized and the optimal procedure of learning is determined (Dai et al, 1998). A method for face recognition using Hopfield memory model combined with the pattern matching is proposed. It shows better performance of database having faces of 40 subjects.

A Hierarchical Neural Network

It is grown automatically and not trained with gradient descent was used for face recognition by (Weng *et al.* 1995). They reported good results for discrimination of ten subjects. The ability of the compression networks was demonstrated by Cottrell and Fleming in Cottrell *et al.* (1990). In Valentin *et al.* (1994), linear autoassociative networks, nonlinear autoassociative (or compression) and/or hetero-associative back propagation networks are explored for face processing. Lin *et al.* (1997) proposed a face

recognition technique based on Probabilistic Decision based Neural network (PDBNN). It adopts a hierarchical network structures with nonlinear basis functions and competitive credit assignment scheme. It demonstrated a successful application of PDBNN on FERET and ORL databases.

Recently, Gutta *et al.* (2000) described the application of mixtures of experts on gender and ethnic classification of human faces and pose classification and showed their feasibility on the FERET database. The mixture consists of ensembles of radial basis functions (RBFs). Inductive Decision Trees (IDTs) and SVMs implement the "gating network" components for deciding which of the experts should be used to determine the classification output and to restrict the support of the input space. Experimental results yield good results on gender, ethnic and pose classification, which can be effectively used in face recognition.

2.6.4 Hybrid Approach

This type of approach uses both statistical pattern recognition techniques and neural networks.

PCA and RBF: The method by Er *et al.* (1999) suggests the use of RBF on the data extracted by discriminant eigenfeatures. They used a hybrid learning algorithm to decrease the dimension of the search space in the gradient method, which is crucial on optimization of high dimension problem. First, they tried to extract the face features by both PCA and LDA methods. Next, they presented a hybrid learning algorithm to train

the RBF Neural Networks, so the dimension of the search space is significantly decreased in the gradient method.

Thomaz *et al.* (1998) also studied on combining PCA and RBF neural network. Their system for face recognition consists of a PCA stage which inputs the projections of a face image over the principal components into a RBF network acting as a classifier.

2.6.5 Geometry Feature Based Methods

Geometry feature based methods uses the facial feature measures such as distance between eyes, ratio of distance between eyes and nose, but it is significantly different from the feature-based techniques that it constructs the topological graph using the facial features of each subject.

Graph Matching Based Methods: In Lades *et al.* (1997), the authors presented a dynamic link architecture for distortion invariant object recognition which employs elastic graph matching to find the closed stored graph. Objects were represented with sparse graphs whose vertices were labelled with geometrical distances. In this system, individual faces were represented by a rectangular graph, each node labelled with a set of complex Gabor wavelet coefficients, called a jet. Only the magnitudes of the coefficients were used for matching and recognition. When recognizing a face of a new image, each graph in the model database was matched to the image separately and the best match indicated the recognized person. They presented good results with a database of 87 subjects and test images composed of different expressions and faces turned 15 degree.

The matching process was computationally expensive, taking roughly 25 seconds to compare an image with 87 stored objects when using a parallel machine with 23 transputers.

Wiskott *et al.* (1997) extended this system to handle larger galleries and larger variations in pose and to increase the matching accuracy. Firstly, they use the phase of the complex Gabor wavelet coefficients to achieve an accurate location of the nodes and to disambiguate patterns which would be similar in the magnitudes of the coefficient. Secondly, they employ object adapted graphs, so that nodes refer to specific facial landmarks, called fiducial points. The correspondences between two faces can be found across large viewpoint changes. Thirdly, a new data structure called the bunch graph was introduced which serves as generalized representation of faces by combining jets of a small set of individual faces. This allows the system to find the fiducial points in one matching process, which eliminates the need for matching each model graph individually. This also reduces computational effort significantly. It offers good performance of about 98% for FERET database. But the drawback in this feature matching approach is that it requires manual intervention to select the fiducial points in the facial image and it requires precise location of those points.

Feature Based PCA: Cagnoni and Poggi suggested a feature based approach instead of a holistic approach to face recognition. They applied the eigenface method to sub-images

(eye, nose and mouth). They also applied a rotation correction to the faces in order to obtain better results, Cagnoni *et al.* (1999).

2.6.6 Other Approaches

Range Data: One of the different methods used in face recognition task is using the range images. In this method data is obtained by scanning the individual with a laser scanner system. This system also has the depth information so the system processes 3-dimensional data to classify face images (Chellappa *et al.* 1995).

Infrared Scanning: Another method used for face recognition is scanning the face image by an infrared light source. Yoshitomi *et al.* (1997) used thermal sensors to detect temperature distribution of a face. In this method, the front view face in input image is normalized in terms of location and size, followed by measuring the temperature distribution, the locally averaged temperature and the shape factors of face. The measured temperature distribution and the locally averaged temperature are separately used as input data to feed a neural network and supervised classification is used to identify the face. The disadvantage of visible ray image analysis is that the performance is strongly influenced by lighting condition including variation of shadow, reflection and darkness. These can be overcome by the method using infrared rays.

Profile Images: Liposcak and Loncaric, Liposcak *et al.* (1999), worked on profile images instead of frontal images. Their method is based on the representation of the original and morphological derived profile images. Their aim was to use the profile

outline that bounds the face and the hair. They take a gray-level profile image and threshold it to produce a binary image representing the face region. They normalize the area and orientation of this shape using dilation and erosion. Then, they simulate hair growth and haircut and produce two new profile silhouettes. From these three profile shapes they obtain the feature vectors. After normalizing the vector components, they use the Euclidean distance measure for measuring the similarity of the feature vectors derived from different profiles.

2.6.7 Face Recognition using Principal Component Analysis

Previous mathematicians (Turk and Pentland, 1999), have theorised that certain cognitive processes, such as face recognition, can be emulated through the use of principal component analysis. Principal component analysis (PCA) is a statistical dimensionality reduction method, which produces the optimal linear squares decomposition of a training set. It reduces the dimensionality of a data set while retaining the majority of the variation present in the data set (Jolliffe, 1986).

PCA is a mathematical procedure that uses an orthogonal transformation to convert a set of observations of possibly correlated variables into a set of values of uncorrelated variables called principal components. The number of principal components is less than or equal to the number of original variables. This transformation is defined in such a way that the first principal component has as high a variance as possible (that is, accounts for as much of the variability in the data as possible), and each succeeding component in turn

has the highest variance possible under the constraint that it be orthogonal to (uncorrelated with) the preceding components. Principal components are guaranteed to be independent only if the data set is jointly normally distributed. PCA is sensitive to the relative scaling of the original variables. Depending on the field of application, it is also named the discrete Karhunen–Loève transform, the Hotelling transform or proper orthogonal decomposition.

PCA was invented in 1901 by Karl Pearson. Now it is mostly used as a tool in exploratory data analysis and for making predictive models. PCA can be done by eigenvalue decomposition of a data covariance matrix or singular value decomposition of a data matrix, usually after mean centring the data for each attribute. The results of a PCA are usually discussed in terms of component scores (the transformed variable values corresponding to a particular case in the data) and loadings (the variance each original variable would have if the data were projected onto a given PCA axis) (Shaw, 2003).

PCA is the simplest of the true eigenvector-based multivariate analyses. Often, its operation can be thought of as revealing the internal structure of the data in a way which best explains the variance in the data. If a multivariate dataset is visualised as a set of coordinates in a high-dimensional data space (1 axis per variable), PCA can supply the user with a lower-dimensional picture, a "shadow" of this object when viewed from its (in some sense) most informative viewpoint. This is done by using only the first few principal components so that the dimensionality of the transformed data is reduced.

It has been successfully used in face recognition systems. In the case of face recognition system based on PCA, it seeks to capture the variation in a collection of face images and use this information to encode and compare images of individual faces in a holistic manner. Eigen–face method is verified well for the recognition strategy and in controlled condition.

An image space can be considered as a space having dimensions equal to the number of pixels making up the image and having values in the range of the pixels values. An image can be thought as a point in the image space by converting the image to a long vector by concatenating each column of the image one after the other (Bahtiyar, 1998).

When all the face images are converted into vectors, they will group at a certain location in the image space as they have similar structure, having eye, nose and mouth in common and their relative position correlated. This correlation is the main point to start the eigen–face analysis.

The eigen–face method tries to find a lower dimensional space for the representation of the face images by eliminating the variance due to non-face images; that is, it tries to focus on the variation just coming out of the variation between the face images. So eigen–face method aims to build a face space which better describes the faces. The basis vectors of this face space are called the principal component and the eigen–face method is the implementation of PCA over images.

The fundamental idea behind principal component analysis with eigenvectors has its basis in linear algebra. Put simply, if there are a series of multi-dimensional vectors representing objects which have similarities, it is possible to use a transformation matrix and eigenvectors to orient a space which requires fewer dimensions to accurately describe these multidimensional vectors.

Eigen-faces for Recognition

In the language of information theory, we want to extract the relevant information in a face image, encoding with a database of models encoded similarly as efficiently as possible, and compare one face encoding with a database of models, encoded similarly. So, mathematically we wish to find the principal components of the distribution of faces, or the eigen–vectors of the covariance matrix of the set of face images.

A simple approach to extract the information contained in an image of a face is to somehow capture the variation in a collection of face images, independent of any judgment of features, and use this information to encode and compare individual face images.

In mathematical terms, eigen–face method finds the principal components of the distribution of faces, or the eigen–vectors of the covariance matrix of the set of face images, treats an image as point (or vector) in a very high dimensional space. The eigen-vectors are ordered, each one accounting for a different amount of the variation among the face images (Turk and Pentland, 1999).

These eigen–vectors can be thought of as a set of features that together characterize the variation between face images. Each image location contributes more or less to each eigen–vector, so that we can display the eigen–vector as a sort of ghostly face which is why we call this by eigen–face. Each eigen–face deviates from uniform gray where some facial feature differs among the set of training faces; they are a sort of map of the variations between faces. Each individual face can be represented exactly in terms of a linear combination of the eigen–faces.

The number of possible eigen-faces is equal to the number of face images in the training set. However we can also represent the faces by approximating these by the best eigen–faces having largest eigen–values which in turn account for the most variance within the set of face images. This increases the computational efficiency.

The information theory approach of encoding and decoding face images extracts the relevant information in a face image, encode it as efficiently as possible and compare it with database of similarly encoded faces. The encoding is done using features which may be different or independent than the distinctly perceived features like eyes, ears, nose, lips, and hair.

Mathematically, principal component analysis approach will treat every image of the training set as a vector in a very high dimensional space. The eigenvectors of the covariance matrix of these vectors would incorporate the variation amongst the face images. Now each image in the training set would have its contribution to the

eigenvectors (variations). This can be displayed as an '*eigenface*' representing its contribution in the variation between the images.

CHAPTER THREE

METHODOLOGY

A FACE–BASED ATM IDENTIFICATION SECURITY MODEL

The high dimensional space with all the eigenfaces is called the image space (feature space). Also, each image is actually a linear combination of the eigenfaces. The amount of overall variation that one eigenface counts for, is actually known by the eigenvalue associated with the corresponding eigenvector. If the eigenface with small eigenvalues are neglected, then an image can be a linear combination of reduced number of these eigenfaces. For example, if there are M images in the training set, we would get M eigenfaces. Out of these, only M' eigenfaces are selected such that they are associated with the largest eigenvalues. These would span the M'–dimensional subspace 'face space' out of all the possible images (image space).

The following steps are involved in the recognition process (Turk and Pentland, 1999): (i) initialisation: The training set of face images is acquired and eigen-faces are calculated which define the face space; (ii) when a new face is encountered, a set of weights based on input image and M eigen-faces is calculated by projecting the input image onto each of the eigen-faces; (iii) the image is determined to be a face or not by checking if it is sufficiently close to face space; and (iv) if it is a face, the weight patterns are classified as either a known person or an unknown one.

3.11 Construction of face space

A face, which is an image, can be viewed as a vector. If the image's width and height are *w* and *h* pixels respectively, the number of components of this vector will be *w*h*. Each pixel is coded by one vector component. The construction of this vector from an image is performed by a simple concatenation – the rows of the image are placed each beside one another, as shown on the Fig. 3.1. The main idea of the PCA is to find the vectors which best account for the distribution of face images within the entire image space.

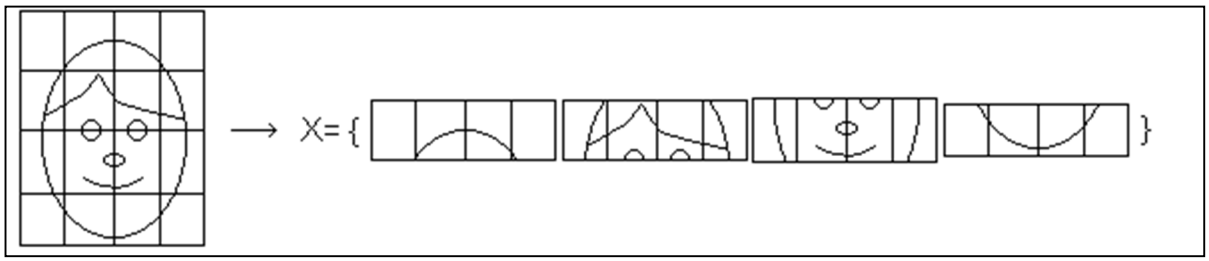


Fig. 3.1 – Formation of the face's vector from the face's image

To create a set of eigenfaces, one must:

(i) Prepare a training set of face images. The pictures constituting the training set should have been taken under the same lighting conditions, and must be normalized to have the eyes and mouths aligned across all images. They must also be all resampled to the same pixel resolution. Each image is treated as one vector, simply by concatenating the rows of pixels in the original image, resulting in a single row with $r \times c$ elements where r is... c. For this implementation, it is assumed that all images of the training set are stored in a single matrix *T*, where each row of the matrix is an image.

(ii) Subtract the mean. The average image *a* has to be calculated and then subtracted from each original image in *T*.

(iii) Calculate the eigenvectors and eigenvalues of the covariance matrix S. Each eigenvector has the same dimensionality (number of components) as the original images, and thus can itself be seen as an image. The eigenvectors of this covariance matrix are therefore called eigenfaces. They are the directions in which the images differ from the mean image. Usually this will be a computationally expensive step (if at all possible), but the practical applicability of eigenfaces stems from the possibility to compute the eigenvectors of S efficiently, without ever computing S explicitly.

(iv) Choose the principal components. The D x D covariance matrix will result in D eigenvectors, each representing a direction in the $r \times c$-dimensional image space. The eigenvectors (eigenfaces) with largest associated eigenvalue are kept.

These eigenfaces can now be used to represent both existing and new faces: we can project a new (mean–subtracted) image on the eigenfaces and thereby record how that new face differs from the mean face. The eigenvalues associated with each eigenface represent how much the images in the training set vary from the mean image in that direction. We lose information by projecting the image on a subset of the eigenvectors, but we minimize this loss by keeping those eigenfaces with the largest eigenvalues. For instance, if we are working with a 100 x 100 image, then we will obtain 10,000 eigenvectors. In practical applications, most faces can typically be identified using a projection on between 100 and 150 eigenfaces, so that most of the 10,000 eigenvectors can be discarded.

Suppose a face image consists of N pixels, so it can be represented by a vector Γ of dimension N. Let$\{\Gamma_i | i = 1, \ldots, M\}$ be the training set of face images. The average face of these M images is given by

$$\Psi = \frac{1}{M}\sum_{i=1}^{M}\Gamma_i \qquad (3.1)$$

Then each face Γ_i differs from the average face Ψ by Φ_i:

$$\Phi_i = \Gamma_i - \Psi;\ i = 1, \ldots, M \qquad (3.2)$$

A covariance matrix of the training images can be constructed as follows:

$$C = AA^T \qquad (3.3)$$

where A= $[\Phi_1, \ldots, \Phi_M]$. The basis vectors of the face space, i.e., the eigenfaces, are then the orthogonal eigenvectors of the covariance matrix C.

Finding the eigenvectors of the N by N matrix C is an intractable task for typical image sizes, hence, a simplified way of calculation has to be adopted. Since the number of training images is usually less than the number of pixels in an image, there will be only M–1, instead of N, meaningful eigenvectors. Therefore, the eigenfaces are computed by first finding the eigenvectors, v_l ($l = 1, \ldots, M$), of the M x M matrix L:

$$L=A^TA. \qquad (3.4)$$

The eigenvectors, u_l ($l = 1, \ldots, M$), of the matrix C are then expressed by a linear combination of the difference face images, Φ_i ($i = 1, \ldots, M$) , weighted by v_l ($l = 1, \ldots, M$):

$$U = [u_1, \ldots, u_M] = [\Phi_i, \ldots, \Phi_M][v_i, \ldots, v_M] = A.V \qquad (3.5)$$

In practice, a smaller set of M' (M' < M) eigenfaces is sufficient for face identification. Hence, only M' significant eigenvectors of L, corresponding to the largest M' eigenvalues, are selected for the eigenface computation, thus resulting in a further data compression. M' is determined by a threshold, θ_λ, of the ratio of the eigenvalue summation:

$$M' = \min_r \left\{ r \mid \frac{\sum_{I=1}^{r} \lambda_I}{\sum_{I=1}^{M} \lambda_I} > \theta_\lambda \right\}. \qquad (3.6)$$

(i) Face recognition using eigenfaces

The eigenface–based face recognition procedure is composed of two stages: a training stage and a recognition stage.

In the training stage, the face of each known individual, Γ_k, is projected into the face space and an M'-dimensional vector, Ω_k, is obtained:

$$\Omega_k = U^T(\Gamma_k - \Psi); k = 1, \ldots, N_c, \qquad (3.7)$$

Where N_c is the number of face classes.

A distance threshold, θ_c, that defines the maximum allowable distance from a face class as well as from the face space, is set up by computing half the largest distance between any two face classes:

$$\theta_c = \frac{1}{2} \max_{j,k} \{ \|\Omega_j - \Omega_k\|; j, k = 1, \ldots, N_c \}. \qquad (3.8)$$

In the recognition stage, a new image, Γ, is projected into the face space to obtain a vector, Ω:

$$\Omega = U^T \Gamma - \Psi. \qquad (3.9)$$

The distance of Ω to each face class is defined by

When the face image to be recognised (known or unknown), is projected on this faces-pace (Fig.3.2), we get the weights associated with the eigenfaces, that linearly approximate the face or can be used to reconstruct the face (Yu et. al., 1997). Now these weights are compared with the weights of the known face images so that it can be recognized as a known face used in the training set. In simpler words, the Euclidean-distance between the image projection and known projections is calculated; the face image is then classified as one of the faces with minimum Euclidean distance.

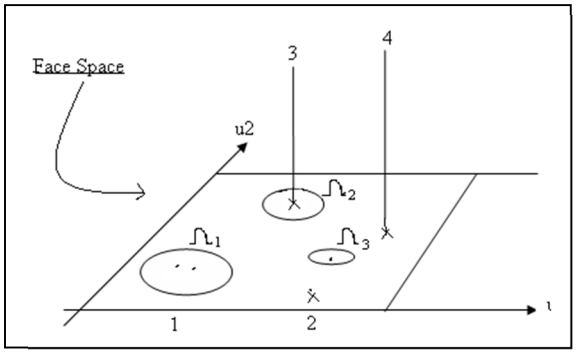


Fig. 3.2 - The face space (u1 and u2 are the eigenfaces).

For the purpose of discriminating between face images and non-face like images, the distance, ε, between the original image, Γ, and its reconstructed image from the eigenface space, Γ_f, is also computed:

$$\varepsilon^2 = \|\Gamma - \Gamma_f\|^2, \quad (3.11)$$

where

$$\Gamma_f = U.\Omega + \Psi. \quad (3.12)$$

These distances are compared with the threshold given in equation (3.8) and the input image is classified by the following rules:

IF $\varepsilon \geq \theta_c$ THEN

input image is not a face image;

IF $\varepsilon < \theta_c$ AND $\forall k, \varepsilon_k \geq \theta_c$ THEN

input image contains an unknown face;

IF $\varepsilon < \theta_c$ AND $\varepsilon_{k^*} = \min_k\{\varepsilon_k\} < \theta_c$ THEN

input image contains the face of individual k^*.

3.2 Architecture of a face-based secure ATM identification security system

Face recognition refers to a very broad range of applications including secure access control, crowd surveillance, forensic facial reconstruction and police identification. Many systems are today commercially available, for instance, one can name several 2D systems developed by Cognitec Systems GmbH, Neven Vision, Viisage, and Indentix. More recently, there has been an emergence of 3D face recognition systems e.g. A4Vision, Geometrix, and Genex Technologies. All these systems belong to the category of static face recognition, and there exists currently no solution that exploits the idiosyncrasies of facial expressions for person identification.

The identification problem is a one-to-many comparison in which the probe v_Q of an unknown person is compared to all biometric templates $\{(I_k,v_k),k = (1,...,N)\}$ of known subjects enrolled in the database. The face identification problem can be formally posed as follows: given a probe v_Q of an unknown person, determine the identity I_i, $i \in \{1, 2,...,N, N+1\}$ where $I_1,I_2,...,I_N$ are the identities enrolled in the database and I_{N+1} indicates the reject case where no suitable identity can be determined for the user. Thus:

$$v_Q \in \begin{cases} I_i \; if \; \max_i S(v_Q, v_i) \geq t, i = 1,2,...,N \\ I_{N+1}, otherwise \end{cases}$$

Where v_i is the biometric template corresponding to identity I_i, S is the function that measures the similarity between v_Q and v_i, and t is a predefined threshold. Since biometric samples of the same individual taken at different times are almost never identical (due to different imaging conditions or different interactions between the user and the system, for example), it is difficult to determine the perfect match. Thus, instead of reporting a unique identity I_i, the system outputs a set of possible matches which can be determined in two ways: threshold-based or rank-based. The main modules of a face identification system are as shown in fig. 3.3.

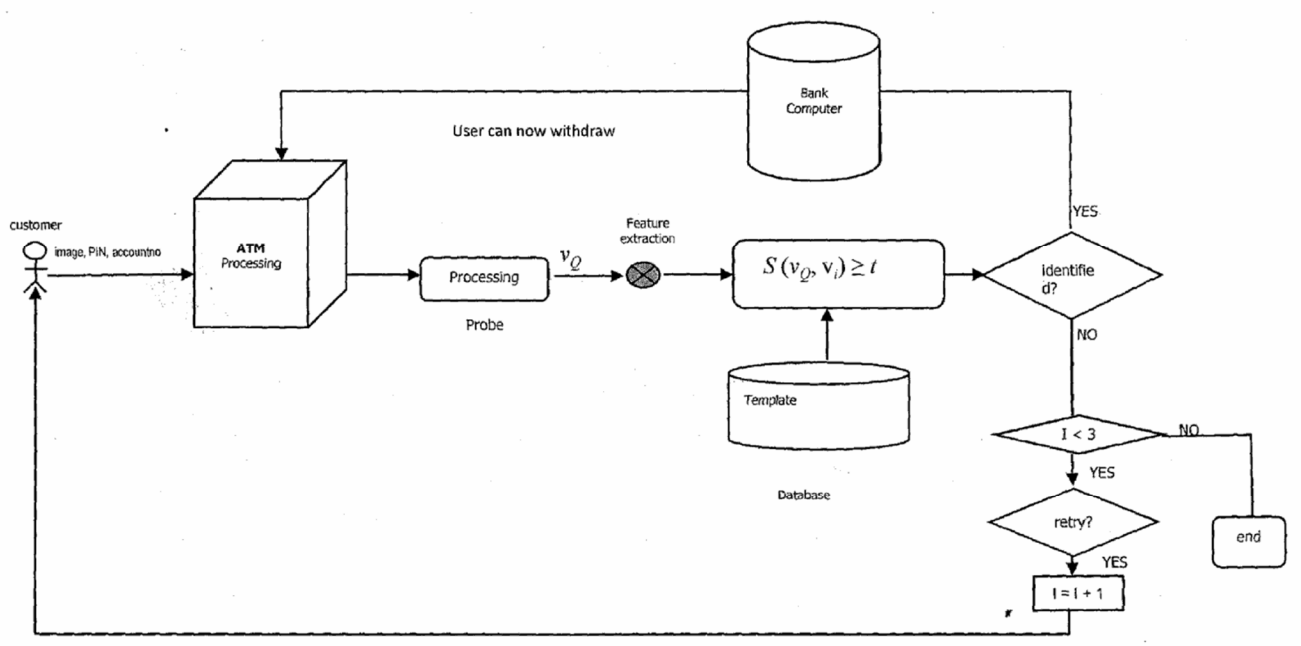


Fig. 3.3: Main modules in a face identification system.

Face identification: the probe v_Q of an unknown user is matched against all biometric templates v_i in the database to determine his/her identity.

In a threshold-based mode, t is preset by the constructor according to the security level required. If t is too large, the system may fail to identify many users. If t is too small, the system will output a large number of possible matches, many of these are inaccurate.

The more common approach to design an identification system is the rank based mode. The system typically determines a set of m best matches which present the highest matching scores. m is usually referred to as the rank. The system always returns a fixed number of outputs: the m known identities enrolled in the database who resemble the most to the unknown user, sorted in some order. The UML (Unified Modelling Language), sequence diagram of the recognition face is as shown in the fig. 3.4.

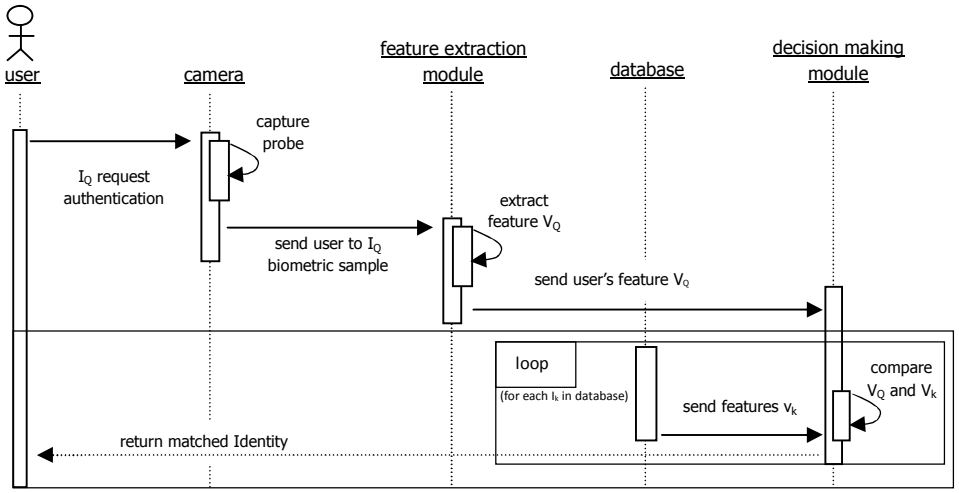


Fig. 3.4: Unified Modelling Language sequence diagram of the recognition process.

3.3 Software Requirement

For most of the past ten years, the majority of ATMs used worldwide ran under IBM's now-defunct OS/2. However, IBM hasn't issued a major update to the operating system in over six years. Movement in the banking world is now going in two directions: Windows and Linux. National Cash Register (NCR), a leading world-wide ATM manufacturer, recently announced an agreement to use Windows XP Embedded in its next generation of personalized ATMs *(crmdaily.com.)* Windows XP Embedded allows OEMs to pick and choose from the thousands of components that make up Windows XP Professional, including integrated multimedia, networking and database management functionality. This makes the use of off-the-shelf facial recognition code more desirable because it could easily be compiled for the Windows XP environment and, the networking and database tools will already be in place.

Many financial institutions are relying on Windows NT, because of its stability and maturity as a platform. The ATMs send database requests to bank servers which do the bulk of transaction processing *(linux.org.)* This model would also work well for the proposed system if the ATMs processors were not powerful enough to quickly perform the facial recognition algorithms.

CHAPTER FOUR

SYSTEM IMPLEMENTATION

4.1 Introduction

There is an urgent need for improving security in banking region. With the advent of ATM, banking became a lot easier and a lot more vulnerable. The chances of misuse of this much hyped 'insecure' ATM are manifold due to the exponential growth of 'intelligent' criminals day by day. ATM systems today use no more than an access card and PIN for identity verification. This model invites fraudulent attempts through stolen cards, badly-chosen or automatically assigned PINs, cards with little or no encryption schemes, employees with access to non-encrypted customer account information and other points of failure.

This chapter presents an automatic teller machine security model that would combine a physical access card, a Personal Identification Number (PIN), and an electronic facial recognition. By forcing the ATM to match a live image of a customer's face with an image stored in a bank database that is associated with the account number, the damage to be caused by stolen cards and PINs is effectively neutralized. Only when the PIN matches the account *and* the live image and stored image match would a user be considered fully verified.

The main issues faced in developing such a model are keeping the time elapsed in the verification process to a negligible amount, allowing for an appropriate level of variation in a customer's face when compared to the database image, and that credit cards which

can be used at ATMs to withdraw funds are generally issued by institutions that do not have in-person contact with the customer, and hence no opportunity to acquire a photo.

When a match is made with the PIN but not the images, the bank could limit transactions in a manner agreed upon by the customer when the account was opened, and could store the image of the user for later examination by bank officials. In regards to bank employees gaining access to customer PINs for use in fraudulent transactions, this system would likewise reduce that threat to exposure to the low limit imposed by the bank and agreed to by the customer on visually unverifiable transactions.

4.2 How the System Works

When a customer puts in an ATM bankcard, a webcam locates the face and takes a digital image of the customer's face. Fig. 4.1 depicts how the system works.

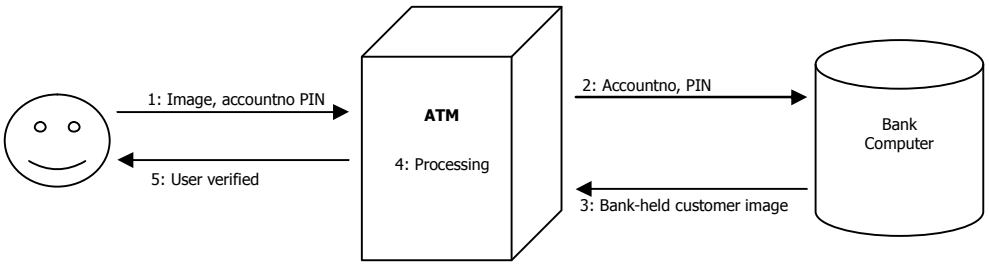


Fig. 4.1 – ATM security model

The system works equally well with customers wearing glasses or contact lenses and at night. No special lighting is needed. When the system is fully operational, a bank customer will have his/face recorded for comparison when an account is opened.

The system consists of typically four basic components:

(i) The Data Acquisition Module

This module comprises the imaging and lighting apparatus necessary for capturing video data of the users. The present application requires an off-the-shelf video camera that needs to be sufficiently fast to accurately capture real-time facial deformations.

Since all dynamic image capture systems today operate within a limited field of vision, they are not suitable for recognition from far distance, e.g. crowd surveillance. For this reason, the present study will focus solely on applications where the users are cooperative e.g. computer login and secure access control. The users are typically required to perform some short verbal or nonverbal facial actions; the recording conditions are designed to model as closely as possible real-life situations.

(ii) The Feature Extraction Module

This module comprises the algorithms necessary for extracting and quantifying facial motion characteristics from videos. At enrolment, facial performances of known persons are collected. This module can be subsequently used to estimate/extract facial dynamics from a given image from camera.

(iii) The Database

This is a database that contains the biometric templates of known persons who are enrolled into the system. Typically, a biometric template is a pair (I_k, v_k) where I_k is a known identity for example name - and v_k is the facial motion signature associated with I_k.

The database can be either centralised or distributed e.g. a smart card carried by each user. The centralised scenario is more efficient to avoid counterfeit or lost cards, but it has to deal with scalability issues. In large-scale systems of thousands of identities, it can be computationally taxing to match the biometric sample of an unknown user – the probe – against all stored biometric templates in the database. In order to reduce the computational overhead of pattern matching, it is usually necessary to classify the templates in the centralised database. For example, if we know that the user is a man, there is no need to check his probe against women's templates.

(iii) The decision making module

This module comprises the pattern matching algorithms necessary for measuring the resemblance between two biometric samples, together with the implementation of the policy related to the matching process. Pattern matching involves comparing a probe of an unknown user to a biometric template in the database. The matching process generates a numerical estimation of the similarity.

A threshold is usually defined by the system constructor, above which the biometric samples are considered as belonging to the same person. The choice of the threshold is a matter of policy. In a high-security application where the cost of a false acceptance could be high, system policy might prefer very few false acceptances and many more false rejections. In a commercial setting where the cost of a false acceptance could be small and treated as a cost of doing business, system policy might favour false acceptances in order not to falsely reject and thereby inconvenience large numbers of legitimate customers.

Once the eigenfaces have been computed, the face space has to be populated with known faces. Usually these faces are taken from the training set. Each known face is transformed into the face space and its components stored in memory.

- **Build face space**
  - PCA
  - Calculate the mean of the input face images
  - Subtract the mean from the input images to obtain the mean-shifted images
  - Calculate the eigevectors and eigenvalues of the mean-shifted images
  - Order the eigenvectors by their corresponding eigenvalues, in decreasing order
  - Retain only the eigenvectors with the largest eigenvalues (*the principal components*)

- Project the mean shifted images into the eigenspace using the retained eigenvectors.

-

- **Project Image Vectors onto Face space**
  - Nearest known face (Euclidean distance) matches
  - Thresholds for distance to face class vs. distance to face space
    - In face space, but no match
    - Not in face space

At this stage the identification process can begin. An unknown face is presented to the system. The system projects it onto the face space and computes its distance from all the stored faces. The face is identified as being the same individual as the face which is nearest to it in face space. There are several methods of computing the distance between multidimensional vectors. Here, a form of Euclidean distance is chosen. In fact it is the cosine of the angle between the two faces which is computed. Since the faces are normalised (vector magnitude equals 1), a comparison of cosine distances and Euclidean distances is identical. The advantage is that cosine distances can be calculated far more efficiently.

The identification process is summarised in Fig. 4.2.

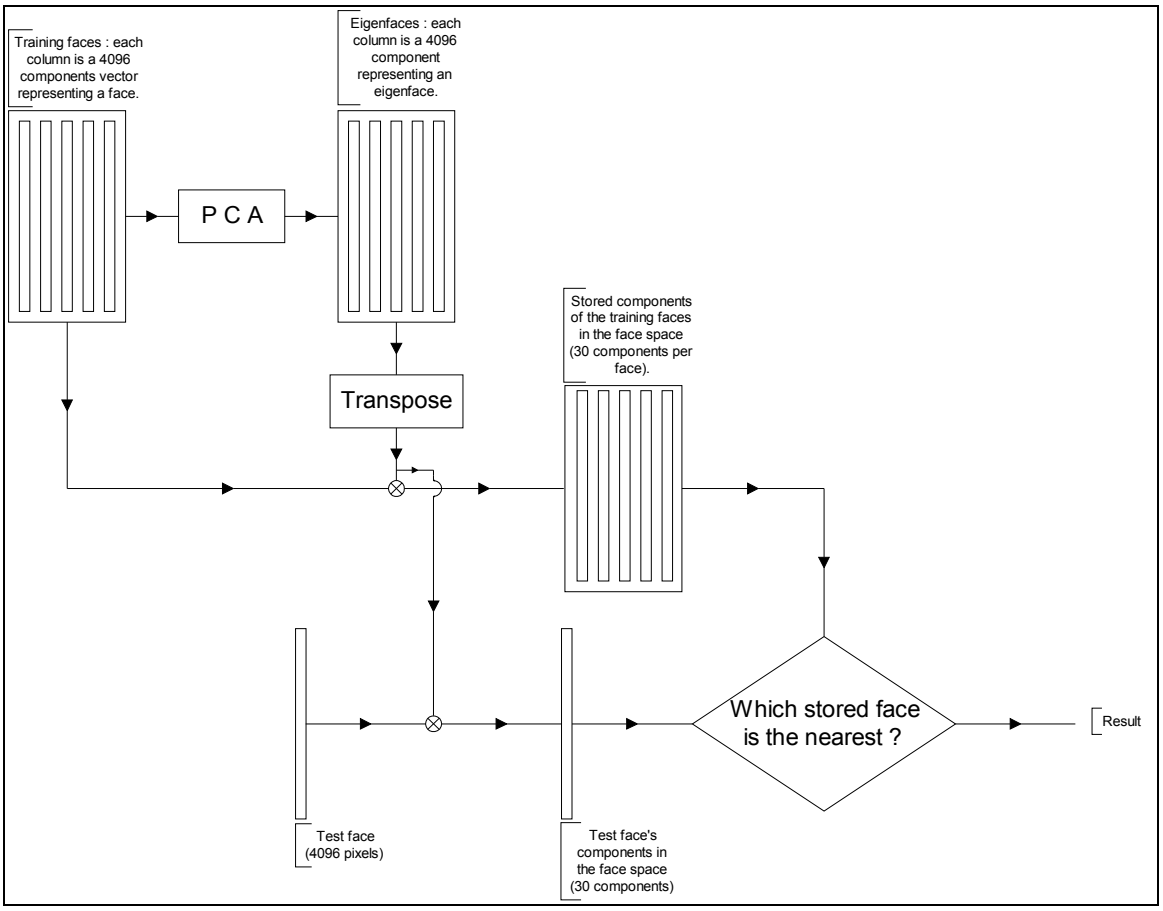


Fig. 4.2 – Identification process

4.3 Development Environment

The specification for the environment where the model was developed and tested is given below

- CPU: INTER (R) Dual CPU
- RAM: 2GB
- OPERATING SYSTEM: WINDOW VISTA
- Programming Language. MATLAB

4.4 Result

customer	identification status	transaction status
	**Identified**	**access granted**
	**Identified**	**access granted**
	**Identified**	**access granted**
	**Identified**	**access granted**
	**Identified**	**access granted**

	**Identified**	**access granted**
	**Identified**	**Access not granted**

Fig 4.3 Pictures used for face recognition.

Access could only be granted if the pictures have been taken with slight variations in pose, lightning conditions and facial expressions the encoding is partially based on the intensity of the images.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

The project aims at an ATM face recognition model for banks as an additional biometric device to the already existing ones. The program written by Luigi Rosa (1991) was adopted and enhanced by me to be able to implement the model that has been designed. The model was designed to verify the customers image at the ATM counter captured at the counter, with the Banks existing customers whose faces have already been captured in the database.

The pictures of seven (7) individuals are taken and stored in the database. For each individual four pictures are taken. All the faces images are basically frontal with some variation in pose angle and distance from camera and constant lighting condition is maintained.

The pictures of the individual constitutes what is known as Class.

The combination of all the classes is known as the face space. For the purpose of verification, the picture taken at the counter at the ATM sends the details of the facial dimensions to the database for verification. The image vector is projected onto the face space. The class with the shortest distance (Euclidean distance) to the image vector is the one that matches with the picture taken at the counter.

Where the distance of the projected image from the class and distance from the facespace is less than the threshold value, the projected image is a known face otherwise it is an unknown face.

The choice of threshold is a matter of policy in a high-security application where the cost of a false acceptance could be high, system policy might prefer very few false acceptances and many false rejection. In a banking environment where the cost of a false acceptance may be small and could be treated as cost of doing business, banks policy might prefer false acceptance in order not to falsely reject and in the process inconvenience and frustrate large numbers of legitimate customers.

- Cameras in use at automatic teller machine take still images of users.
- A facial recognition scheme should be added to the software used to verify users at ATMs.
- This scheme should match a picture of the user at the ATM with a picture of the account holder in the bank's database.

5.2 Conclusion

In this thesis, an ATM model that is more reliable in providing security by using facial recognition approach is presented. By keeping the time elapsed in the verification process to a negligible amount we try to maintain the efficiency of this ATM system to a greater degree.

Eigenfaces are an excellent choice for face recognition system because it is fast, simple and accurate in a constrained environment..

Eigenfaces are extremely sensitive to the environment, lightening and pose.

5.3 Recommendation

It is recommended that banks should take video tapes of all their customers that are engaged in different transactions.

It is highly recommended that Banks especially in Nigeria put the result of this project to practical use.

5.4 Future work

The development of a standard image capturing interface or device is essential to support the ATM system. The present work is only a MODEL. This model can be adapted to work with the common database system used by the bank.

If the new captured face is a woman, comparison can be made only to women faces in the database and if the captured face is a man, comparison can be made to man alone.

This would reduce the time for processing to a significant proportion.

In the application in banks with large database the principle of parallel processing is suggested

In case there are identical or ambiguous situation it might be necessary to confirm the correct decision by an application of an additional biometric device such as fingerprint.

REFERENCES

Arun Abraham Ross (1989) Express Cards Entry Kiosks (Http://Www.Cre.Mso.Edo/~Rossarun/Pubs/Ross Ph.D Thesis_03.Pdf) .

Anil K. Jain and Avon Ross and Salil Prahakar (2004) *an Introduction to Biometric Recognition.* IIEE Journal. Transaction On Circuits and Systems for Video Technology Vol 14 No. 1 Pp 8.

Barkley, J. (1995), "Implementing Role-Based Access Control using Object Technology," First ACM Workshop on Role-Based Access Control, Gaithersburg, Maryland.

Bahtiyar A. Gül, (1998), *Holistic Face Recognition by Dimension Reduction,* Master of Science Thesis, Graduate School of Natural and Applied Sciences. The Middle East Technical University. Pp 28-30.

Belhumeur, P. N; Hespanha, J. P and Kriegman, D. J. (1997), *Eigenfaces versus Fisherfaces: Recognition Using Class Specific Linear Projection.* IEEE Tran. on Pattern Analysis and Machine Intelligence, 19(7):711-720.

Bishop, C. M. (1995), *Neural Networks for a Pattern Recognition.* Oxford University Press Inc., New York. Pp 1.

Brunelli, R and Poggio, P. (1993), *Face Recognition: Features versus Templates*. IEEE Tran. On Pattern Analysis and Machine Intelligence, 15(10):1042-1052.

Chellappa, R; Wilson, C. L and Sirohey, S. (1995), *Human and Machine Recognition of Faces:* A Survey. Proc. of the IEEE, 83(5):705-740.

Cognitec Systems GmbHz Source: http://www.cognitec-systems.de. Last visited December 12, 2010.

Cootes, T. J; Lanitis, A and Taylor, C. J, and (1997), *Automatic Interpretation and Coding of Face Images using Flexible Models.* IEEE Tran. On Pattern Analysis and Machine Intelligence, 19(7):743-756.

Cottrell, G. W and Fleming, M. K. (1990), *Recognition Face using Unsupervised Feature Extraction.* In Int. J. Conf. on Neural Networks, Paris. Pp 322-325.

Curmi J (2010), Speedy Adverts, www.speedadverts.com/S.A Topics/html/Information_security1.html

Dai, Y and Nakano, Y. (1998), *Recognition of Facial Images with Low Resolution using a Hopfield Memory Model.* Pattern Recognition, 31(2):159-167.

Demers, D and Cottrell, G. W. (1993), *Nonlinear Dimensionality Reduction.* In Advances in Neural Information Processing Systems, Pp 580-587.

Diebold Inco. (2002), ATM Fraud Security white paper. (http://banktech.com)

Er, M. J; Wu, S and Lu, J. (1999), *Face Recognition using Radial Basis Function (RBF) Neural Networks.* In 38th Conference on Decision & Control, Phoenix, Arizona USA. Pp Face 2162-2167,

Essinger, J. (1987), *ATM Networks, Their Organization Security and Finance,* published by Elservier Int Bulletin Chp 6 Future developments.

Fan, Ming, (2002) *Computer Sciences › January 2002* - Cached (*www.encyclopedia.com)*

Fenton, M. (2008), by Admin. Banking systems and technology; The Blog. Taking ATM fraud prevention to the next level.

Genex Technologies Inc.," Source: http://www.genextec.com. Last visited December 9, 2010.

Geometrix Inc.," Source: http://www.geometrix.com. Last visited December 9, 2010.

Gutta, S; Huang, J. R. J; Jonathan, P and Wechsler, H. (2000), *Mixture of Experts for Classification of Gender, Ethnic Origin, and Pose of Trans Human Faces.* IEEE. Trans On Neural Networks, 11:948-959.

Hamelink, C. (2000), "The Ethics of Cyberspace," Sage, London, Ind, N. "Living the Brand," Kogan Page, London Pp.

Haykin, S. (1999), *Neural networks: A Comprehensive Foundation.* Prentice-Hall International, New Jersey. Pp 51 and 306.

Howell, A. J and Buxton, H. (1995), *Invariance in Radial Basis Function Neural Networks in Human Face Classification.* Neural Processing Letters, 2(3):26-30.

Huang, J. (1998), *Detection Strategies for Face Recognition Using Learning and Evolution.* PhD thesis, George Mason University.

Jain, Flynn and Ross, 2008 Edited Handbook of Biometrics (http://EN.wikipedia.org/wiki/Biometric)

Jolliffe, I. T. (1986), *Principal component analysis.* New York: Springer; University of Geneva; ISBN: 0-387-96269-7.

Jøsang, A and Pope, S, (2005), *User Centric Identity Management,* AusCERT Conference 2005.

Kalakota, R. and Whinston, A. B. (2001), "Electronic Commerce: A Manager's Guide" 2nd Edition, Addison Wesley, Harlow. Pp 415-417

Kohonen, T. (1988), *Self-Organization and Associative Memory.* Springer-Verlag, New York.

Kumar, S. (2010), "Introduction to ISO 8583",

www.codeproject.com/Articles/100084/Introduction-to-ISO-8583.

Lades, M; Vorbruggen, J. C; Buhmann, J; Lange, J; Von ser Malburg, C; Wurtz, R. P and Konen, W. (1997), *Distortion Invariant Object Recognition in the Dynamic Link Architecture.* IEEE Transactions on Computers, 42:300-310.

Lawrence, S. C; Lee Giles; Ah Chung Tsoi, and Andrew D. Back, (1998), *Face Recognition: A Conventional Neural Network Approach.* IEEE Trans. on Neural Networks, 8(1):98-113.

Lawrence, S. C; Lee Giles; Ah Chung Tsoi, and Andrew D. Back. (1997), *Face recognition: A Convolutional Neural Network Approach.* IEEE Trans. on Neural Face Networks, 8(1):98-112.

Liposcak, Z and Loncaric, S. (1999), *Face Recognition from Profiles using Morphological Operations. In International Workshop on Recognition, Analysis, and Tracking of Faces and Gestures in Real-Time Systems,* IEEE Conference Publications Pp 47-52.

M. Watanabe (2005).C*ontactless Palm vein systems* Arun A. Ross. Retrieved from http://www.biometrics.org/bc 2005/Presentations/conference/1%/20Monday%2/19/Post.....2nd June, 2012

Mark CBP (Custom And Border Protection)Pilot (2009), *Validating Travel Document* (http:// Foiarr.Cbp.Gov+ Streaming word. Asp?I=42www.Dhs.Gov)

Mammone, R. J. (1993), *Artificial Neural Networks for Speech and Vision.* Chapman and Hall, Cambridge. Pp 97-113

Marcia Crosland, NCR Corp. (2010), *Consumer behaviour drives innovation in ATM technology*. http://www.atmmarketplace.com – 15 Feb 2010

Neven Vision Inc.," Source: http://www.nevenvision.com. Last visited December 13, 2010.

Osuna, E; Freund, R and Girosi, F.(1997), *Training Support Vector Machines: An Application to Face Detection.* In IEEE Conference on Computer Vision and Pattern Recognition, Pp 193-199.

Penev, P and Atick, J. (1996*), Local Feature Analysis*: A General Statistical Theory for Object Representation. Network: Computation in Neural Systems, 7:477-500.

Poggio, T and Sung, K. K, (1994) *Example-based Learning for View-based Human Face Detection.* ARPA Image Understanding Workshop MIT – Pp 401-414.

RCBC (2007), Rizal Commercial Banking Corporation. Electronic Banking (e-Banking) Consumer protection Policy.

Robert J. B. (1981), *Mechanisms of Human Facial Recognition.* International Journal of Man-Machine Studies, 15(2):137-178.

Schlichter, S. (2007), "Using ATM's abroad" Retrieved from

www.msnbc.com/id/16994358 accessed December 8, 2010.

Scholkopf, B; Smola, A. J and Bernhardt, A. (1998), *Nonlinear Component Analysis as a Kernel Eigenvalue Problem.* Neural Computation, 10(5):1299-1319.

Shang-Hung Lin; Sun-Yuan Kung; and Long ji Lin. (1997), *Face Recognition/Detection by Probabilistic Decision-based Neural Network.* IEEE Trans. on Neural Networks, 8(1):114-131.

Shibboleth Project, (2004), *Shibboleth Architecture Protocols and Profiles.* Working Draft 05, 23. Internet2/MACE.

Sirovich, L and Kirby, M. (1987), *Low-dimensional Procedure for the Characterization of Human Faces.* Journal of Optical Society of America, 4(3):519-524.

Stonham, T. J. (1984), *Practical Face Recognition and Verification with WISARD*. In Aspects of Face Processing, Pp 426-441.

Thiagarajan, V. (2002), *Information Security Management,* BS 7799.2:2002, Audit Check List for SANS Institute, BS 7799 Audit Checklist.

Thomas, C. E; Feitosa, R. Q and Veiga, A. (1998), *Design of Radial Basis Function Network as Classifier in face Recognition using Eigenfaces.* In V*th* Brazilian Symposium on Neural Networks, Pp 118-123.

Turk, M and Pentland, A. P. (1991). *Eigenfaces for Recognition*. Journal of Cognitive Neuroscience, 3(1):71-86.

Turk, M. A and Pentland, A. P, (1999), *Face Recognition Using Eigenfaces,* Vision and Modeling Group, the Media Laboratory Massachusetts Institute of Technology.

Valentine, D; Abdi, H; O'Toole, A. J and Cottrell, A. W. (1994), *Connectionist Models of Face Processing:* A survey. Pattern Recognition, 27(9):1209-1230.

Vladimir N. Vapnik. (1995), *The Nature of Statistical Learning Theory.* Springer Verlog, Heidelberg, DE, Pp 188.

Weng, J; Ahuja, N and Huang. T. S. (1995), *Learning Recognition Segmentation of 3-D Objects from 2-D Images.* In Int. Workshop Face Gesture Recognition, Zurich, Switzerland, Pp 403-411.

Wiskott, L; Fellous, J; Kruger, N and Christoph von der Malsburg. (1997), *Face Recognition by Elastic Bunch Graph Matching.* IEEE Tran. on Pattern Analysis and Machine Intelligence, 19(7):775-779.

Wood, P. (2005), "Implementing identity management security - an ethical hacker's view", Network Security, Volume 2005, Issue 9, Pp 12-15.

Yang, M. H, (2002), *Kernel Eigenfaces vs. Kernel Fisherfaces: Face Recognition using Kernel Methods.* In IEEE International Conference on Face and Gesture Recognition, Washington Pp 215-220,

Yegnanarayana, B. (1999), *Artificial Neural Networks.* Prentice-Hall of India, New Delhi. Pp 15-39.

Yoshitomi, Y; Tomito, M. S and Kimura, S (1997), *Face Identification using Thermal Image Processing.* In IEEE International Workshop on Robot 154 and Human Communication, Pp 374-379.

Yu, M; Yan, G and Zhu, Q. (1997*), New Face Recognition Method Based on DWT/DCT Combined Feature Selection,* School of Computer Science, Hebei University of Technology, China.

Yuille, Alan L. (1991), *Deformable Templates for Face Recognition*. Journal of Cognitive Neuroscience, 3(1):59-70.

APPENDIX A: CREATING AND RUNNING THE PROJECT WORK

MENU OF PREVIOUS PROGRAMME WRITTEN FOR FACE RECOGNITION

BY

LUGI ROSA

FACE RECOGNITION SYSTEM
SELECT IMAGE
ADD SELECTED IMAGE TO DATABASE
DATABASE INFO
FACE RECOGITION
DELETE DATABASE
INFO
VISUALIZATION TOOLS
SOURCE CODE FOR FACE RECOGNITION
EXIT

MENUS FOR MODIFICATION OF PREVIOUS PROGRAMME TO IMPLEMENT THE MODEL

A.

FRED KAYODE FACE RECOGNITION SYSTEM
LOADING AND MAINTENANCE OF DATABASE
CAPTURE AND SAVE CUSTOMERS' IMAGE AS PGM
DELETE FACE DATABASE
DATABASE INFO
INFO
VISUALIZATION TOOL
EXIT

B.

FRED KAYODE ATM AUTHENTICATION SYSTEM
VALIDATE CUSTOMER
EXIT

The whole programme consists of two parts namely:

PART A: BACK-END ACTIVITIES

- Taking the photo
- Reducing image size
- Converting image to pgm
- Adding image to database

PART B: FRONT-END ACTIVITIES

- Taking photo
- Verifying face recognition
- Declaring results

The previous programme has database with already stored images from where a choice can be made for face recognition. While the modified version consists of the back-end and front-end activities, the activities available to the customer at the counter are the front-end activities. The front-end activities assume that pictures has already been taken and stored into the bank database. At the counter, pictures of customers are taken from the stationed camera in order to grant the customer access or deny him access to the claimed account.

For face recognition a fresh picture can be taken using the webcam and face recognition can be carried out.

ACTIVATING MENU

To activate the previous menu, do the following;

1. Double-click Matlab icon on the desktop
2. Go to the current work directory
3. Type facerec at the prompt.
4. Press the enter key.

To activate the modified menu, do the following;

A.

1. Double-click Matlab icon on the desktop
2. Go to C:\facerec-
3. Type KAYODFACEREC at the prompt
4. Press the enter key.

B.

1. Double-click Matlab icon on the desktop
2. Go to C:\facerec-
3. Type Alabifacerec at the prompt
4. Press the enter key.

APPENDIX B: SOURCE CODE

PREVIOUS FACE RECOGNITION SYSTEM

BY LUGI ROSA

```
%FACE RECOGNITION SYSTEM
%
% Face recognition system based on EigenFaces Method.
% The system functions by projecting face images onto a feature space
% that spans the significant variations among known face images. The
% significant features are known as "eigenfaces" because they are the
% eigenvectors (principal components) of the set of faces.
%
% Face images must be collected into sets: every set (called "class") should
% include a number of images for each person, with some variations in
% expression and in the lighting. When a new input image is read and added
% to the training database, the number of class is required. Otherwise, a new
% input image can be processed and confronted with all classes present in
database.
% We choose a number of eigenvectors M' equal to the number of classes (see
% algorithmic details in the cited references). Before start image
% processing first select input image. This image can be succesively added to
% database (training) or, if a database is already present, matched with
% known faces.
%
% The images included are taken from AT&T Laboratories Cambridge's
% Face DataBase. See the cited references for more informations.
%
%
% FUNCTIONS
%
% Select image:                                 read the input image
%
% Add selected image to database:               the input image is added to
database and will be used for training
%
% Database Info:                                show informations about the
images present in database. Images must
%                                               have the same size. If this
is not true you have to resize them.
%
% Face Recognition:                             face matching. The selected
input image is processed
%
% Delete Database:                              remove database from the
current directory
%
% Info:                                         show informations about this
software
%
% Visualization tool:                           visualization utility
```

```
%
% Source code for Face Recognition System:       how to obtain the complete
source code
%
% Exit:                                          quit program
%
%
%  References:
%  "Eigenfaces for Recognition", Matthew Turk and Alex Pentlad
%  Journal of Cognitive Neuroscience pp.71-86, March 1991
%  Vision and Modeling Group, The Media Laboratory
%  Massachusetts Institute of Technology.
%  This paper is available at http://www.cs.ucsb.edu/~mturk/Papers/jcn.pdf
%  See also Matthew Turk's homepage
http://www.cs.ucsb.edu/~mturk/research.htm
%
%  AT&T Laboratories Cambridge. The ORL face database, Olivetti Research
Laboratory available at
%  http://www.uk.research.att.com/pub/data/att_faces.zip
%  or http://www.uk.research.att.com/pub/data/att_faces.tar.Z
%
%
%
%
%*****************************************************************
% Luigi Rosa
%*****************************************************************
%
%

%-----------------------------------------------------------------
clear;
clc;
chos=0;
possibility=9;

messaggio='Insert the number of set: each set determins a class. This set
should include a number of images for each person, with some variations in
expression and in the lighting.';

while chos~=possibility,
    chos=menu('Face Recognition System','Select image','Add selected image to
database','Database Info','Face Recognition','Delete Database','Info',...
        'Visualization tool','Source code for Face Recognition
System','Exit');
    %----------------
    if chos==1,
        clc;
        [namefile,pathname]=uigetfile('*.*','Select image');
        if namefile~=0
            [img,map]=imread(strcat(pathname,namefile));
            imshow(img);
            dimensioni = size(img);
            disp('Input image has been selected.');
```

```
            disp('Now press on "Add selected image to database" button to add
this image to database or,');
            disp('press on "Face Recognition" button to start face
matching.');
        else
            warndlg('Input image must be selected.',' Warning ')
        end
    end
    %----------------
    if chos==2,
        clc;
        if exist('img')
            if (exist('face_database.dat')==2)
                load('face_database.dat','-mat');
                face_number=face_number+1;
                data{face_number,1}=img(:);
                prompt={strcat(messaggio,'Class number must be a positive
integer <= ',num2str(max_class))};
                title='Class number';
                lines=1;
                def={'1'};
                answer=inputdlg(prompt,title,lines,def);
                zparameter=double(str2num(char(answer)));
                if size(zparameter,1)~=0
                    class_number=zparameter(1);
                    if
(class_number<=0)||(class_number>max_class)||(floor(class_number)~=class_numb
er)||(~isa(class_number,'double'))||(any(any(imag(class_number))))
                        warndlg(strcat('Class number must be a positive
integer <= ',num2str(max_class)),' Warning ')
                    else
                        if class_number==max_class;
                            max_class=class_number+1;
                        end
                        data{face_number,2}=class_number;

save('face_database.dat','data','face_number','max_class','-append');
                        msgbox(strcat('Database already exists: image
succesfully added to class number ',num2str(class_number)),'Database
result','help');
                        close all;
                        clear('img')
                    end
                else
                    warndlg(strcat('Class number must be a positive integer
<= ',num2str(max_class)),' Warning ')
                end
            else
                face_number=1;
                max_class=1;
                data{face_number,1}=img(:);
                prompt={strcat(messaggio,'Class number must be a positive
integer <= ',num2str(max_class))};
                title='Class number';
                lines=1;
                def={'1'};
                answer=inputdlg(prompt,title,lines,def);
```

```
                zparameter=double(str2num(char(answer)));
                if size(zparameter,1)~=0
                    class_number=zparameter(1);
                    if
(class_number<=0)||(class_number>max_class)||(floor(class_number)~=class_numb
er)||(~isa(class_number,'double'))||(any(any(imag(class_number))))
                        warndlg(strcat('Class number must be a positive
integer <= ',num2str(max_class)),' Warning ')
                    else
                        max_class=2;
                        data{face_number,2}=class_number;

save('face_database.dat','data','face_number','max_class','dimensioni');
                        msgbox(strcat('Database was empty. Database has just
been created. Image succesfully added to class number
',num2str(class_number)),'Database result','help');
                        close all;
                        clear('img')
                    end
                else
                    warndlg(strcat('Class number must be a positive integer
<= ',num2str(max_class)),' Warning ')
                end

            end
        else
            errordlg('No image has been selected.','File Error');
        end
    end
    %----------------
    if chos==3,
        clc;
        close all;
        clear('img');
        if (exist('face_database.dat')==2)
            load('face_database.dat','-mat');
            msgbox(strcat('Database has ',num2str(face_number),' image(s).
There are',num2str(max_class-1),' class(es). Input images must have the same
size.'),'Database result','help');
        else
            msgbox('Database is empty.','Database result','help');
        end
    end
    %----------------
    if chos==4,
        clc;
        close all;
        if exist('img')
            ingresso=double(img(:));
            if (exist('face_database.dat')==2)
                load('face_database.dat','-mat');
                % face_number is equal to "M" of Turk's paper
                % i.e. the number of faces present in the database.
                % These image are grouped into classes. Every class (or set)
should include
                % a number of images for each person, with some variations in
expression and in the
```

```
% lighting.
matrice=zeros(size(data{1,1},1),face_number);
for ii=1:face_number
    matrice(:,ii)=double(data{ii,1});
end
somma=sum(matrice,2);
media=somma/face_number;
for ii=1:face_number
    matrice(:,ii)=matrice(:,ii)-media;
end
matrice=matrice/sqrt(face_number);
% up to now matrix "matrice" is matrix "A" of Turk's paper
elle=matrice'*matrice;
% matrix "elle" is matrix "L" of Turk's paper

% eigenvalues and eigenvectors of the "reduced" matrix  A'*A
[V,D] = eig(elle);
% the following multiplication is performed to obtain the
% eigenvectors of the original matrix A*A' (see Turk's paper)
% See also Karhunen-Loeve algorithm, for face recognition
if det(D)~=0
    Vtrue=matrice*V*(abs(D))^-0.5;
else
    Vtrue=matrice*V;
end
%Vtrue=matrice*V;
Dtrue=diag(D);

% the eigenvalues are sorted by order and only M' of them
% are taken. We impose M' equal to the number of classes
% (max_class-1)
[Dtrue,ordine]=sort(Dtrue);
Dtrue=flipud(Dtrue);
ordine=flipud(ordine);
Vtrue(:,1:face_number)=Vtrue(:,ordine);

Vtrue=Vtrue(:,1:max_class-1);
Dtrue=Dtrue(1:max_class-1);

% we calculate the eigenface components of
% the normalized input (mean-adjusted). I.e. the input
% image is projected into "face-space"
pesi=Vtrue'*(ingresso-media);

pesi_database          = zeros(max_class-1,max_class-1);
pesi_database_mediati  = zeros(max_class-1,max_class-1);

numero_elementi_classe=zeros(max_class-1,1);
for ii=1:face_number
    ingresso_database=double(data{ii,1});
    classe_database=data{ii,2};
    pesi_correnti=Vtrue'*(ingresso_database-media);

pesi_database(:,classe_database)=pesi_database(:,classe_database)+pesi_correnti;
```

```
numero_elementi_classe(classe_database)=numero_elementi_classe(classe_databas
e)+1;
                end
                for ii=1:(max_class-1)

pesi_database_mediati(:,ii)=pesi_database(:,ii)/numero_elementi_classe(ii);
                end
                % pesi_database_mediati is a matrix with the averaged
eigenface components of the images
                % present in database. Each class has its averaged eigenface.
                % We want to find the nearest (in norm) vector to the input
                % eigenface components.

                distanze_pesi=zeros(max_class-1,1);
                for ii=1:(max_class-1)
                    % distanze_pesi(ii)=norm(pesi-
pesi_database_mediati(:,ii));
                    distanze_pesi(ii) = sum((abs(pesi-
pesi_database_mediati(:,ii))));
                end

                [minimo_pesi,posizione_minimo_pesi]=min(distanze_pesi);

                % now we are evaluating the distance of the mean-normalized
                % input face from the "space-face" in order to detrmine if
                % the input image is a face or not.
                proiezione=zeros(size(data{1,1},1),1);
                for ii=1:(max_class-1)
                    proiezione=proiezione+pesi(ii)*Vtrue(:,ii);
                end
                distanza_spazio_facce=norm((ingresso-media)-proiezione);



                messaggio1='See Matlab Command Window to see matching result.
The program has just calculated the minimal distance from classes and the
distance from Face Space. ';
                messaggio2='You now should fix the two threshold-values to
determine if this mathing is correct. If both distances are below the
threshold values it means that the input ';
                messaggio3='face was correctly matched with a known face. If
the distance from Face Space is below the threshold value but the minimal
distance from classes is above the other threshold value, ';
                messaggio4=' it means that the input image is an unknown
face. See the cited article for more informations.';


msgbox(strcat(messaggio1,messaggio2,messaggio3,messaggio4),'Matching
result','help');

                disp('The nearest class is number ');
                disp(posizione_minimo_pesi);
                disp('with a distance equal to ');
                disp(minimo_pesi);
```

```
                disp('The distance from Face Space is ');
                disp(distanza_spazio_facce);



            else
                warndlg('No image processing is possible. Database is
empty.',' Warning ')
            end
        else
            warndlg('Input image must be selected.',' Warning ')
        end
    end
    %----------------
    if chos==5,
        clc;
        close all;
        if (exist('face_database.dat')==2)
            button = questdlg('Do you really want to remove the Database?');
            if strcmp(button,'Yes')
                delete('face_database.dat');
                msgbox('Database was succesfully removed from the current
directory.','Database removed','help');
            end
        else
            warndlg('Database is empty.',' Warning ')
        end
    end
    %----------------
    if chos==6,
        clc;
        close all;
        helpwin facerecexplanation;
    end
    %----------------
    if chos==7,
        clc;
        close all;
        if (exist('face_database.dat')==2)
            load('face_database.dat','-mat');
            disp('Insert 0 to visualize total mean face');
            disp('Insert 1 to visualize class mean face');
            disp('Insert 2 to visualize the projection of input image onto
face-space');
            scelta = input('Insert your choice: ');
            if scelta == 0
                clc;
                matrice=zeros(size(data{1,1},1),face_number);
                for ii=1:face_number
                    matrice(:,ii)=double(data{ii,1});
                end
                somma=sum(matrice,2);
                media=somma/face_number;
                figure('Name','Total mean face');
                imshow(uint8(reshape(media,dimensioni)));
```

```
            end
            if scelta == 1
                clc;
                classescelta = input('Insert class number:');
                if classescelta <= max_class-1
                    somma     = zeros(size(data{1,1},1),1);
                    contatore = 0;
                    for ii=1:face_number
                        if data{ii,2}==classescelta
                            somma = somma + double(data{ii,1});
                            contatore = contatore+1;
                        end
                    end
                    somma = somma/contatore;
                    figure('Name','Class mean face');
                    imshow(uint8(reshape(somma,dimensioni)));
                else
                    warndlg('Class number is uncorrect',' Warning ');
                end
            end
            if scelta == 2
                clc;
                [namefile,pathname]=uigetfile('*.*','Select image');
                if namefile~=0
                    [img,map]=imread(strcat(pathname,namefile));
                    imshow(img);
                    dimensioni = size(img);
                else
                    warndlg('Input image must be selected.',' Warning ')
                end
                ingresso=double(img(:));
                % face_number is equal to "M" of Turk's paper
                % i.e. the number of faces present in the database.
                % These image are grouped into classes. Every class (or set)
should include
                % a number of images for each person, with some variations in
expression and in the
                % lighting.
                matrice=zeros(size(data{1,1},1),face_number);
                for ii=1:face_number
                    matrice(:,ii)=double(data{ii,1});
                end
                somma=sum(matrice,2);
                media=somma/face_number;
                for ii=1:face_number
                    matrice(:,ii)=matrice(:,ii)-media;
                end
                matrice=matrice/sqrt(face_number);
                % up to now matrix "matrice" is matrix "A" of Turk's paper
                elle=matrice'*matrice;
                % matrix "elle" is matrix "L" of Turk's paper

                % eigenvalues and eigenvectors of the "reduced" matrix  A'*A
                [V,D] = eig(elle);
                % the following multiplication is performed to obtain the
                % eigenvectors of the original matrix A*A' (see Turk's paper)
                % See also Karhunen-Loeve algorithm, for face recognition
```

```
                Vtrue=matrice*V*(abs(D))^-0.5;
                %Vtrue=matrice*V;
                Dtrue=diag(D);

                % the eigenvalues are sorted by order and only M' of them
                % are taken. We impose M' equal to the number of classes
                % (max_class-1)
                [Dtrue,ordine]=sort(Dtrue);
                Dtrue=flipud(Dtrue);
                ordine=flipud(ordine);
                Vtrue(:,1:face_number)=Vtrue(:,ordine);

                Vtrue=Vtrue(:,1:max_class-1);
                Dtrue=Dtrue(1:max_class-1);

                % we calculate the eigenface components of
                % the normalized input (mean-adjusted). I.e. the input
                % image is projected into "face-space"
                pesi=Vtrue'*(ingresso-media);


                figure('Name','Projection of inpu image onto face-space');
                imshow(uint8(reshape(Vtrue*pesi+media,dimensioni)))
            end
        else
            warndlg('Database is empty.',' Warning ');
        end
    end
    %----------------
    if chos==8,
        clc;
        close all;
        web http://utenti.lycos.it/matlab/face.htm
        helpwin sourcecode;
    end
end
```

MODIFIED PROGRAM TO LOAD AND MAINTAIN BANK DATABASE

```
%captosavepix.m
%this matlab program captures a cust image with a webcam and save it as
%into the face database
%
% first accept customer ID No (in terms of class, here)...
%
%prompt='Please Enter Your Customer ID No. :';
%title='Enter Customer ID';
%lines=1;
%def={''};
%answer=inputdlg(prompt,title,lines);
%custno=double(str2num(char(answer)));
%
clear;
clc;
chos=0;
possibility=6;
% set cropping values below
%crops = [horz1 vert1 horz2 vert2]
crops = [165 30 320 430]
messaggio='Insert the number of set: each set determins a class. This set
should include a number of images for each person, with some variations in
expression and in the lighting.';

while chos~=possibility,
    chos=menu('Fred Kayode ATM Face Authentication System,loading and
maintenance of database','Capture and Save Customer Image','Delete Face
Database','Database Info','Info',...
        'Visualization tool','Exit');
    %-----------------
    if chos == 1                %capture and save face in database
                % define video input object...to link matlab to the webcam
            f=videoinput('winvideo',2);
            % display the webcam capture window and capture the snapshot
image
            preview(f);
            waitfor(msgbox('Click OK to Capture Your Image','Capture
Image','help'));
            % snap an image shot with the video input object defined above...
            frame = getsnapshot(f);
            % close the preview window
            closepreview(f);
            imshow(frame);
            % next crop the image to a pre-defined size
            img = imcrop(frame, crops)
            imwrite(img, 'custpix.pgm');
            img = imread('custpix.pgm')
            % display the cropped image in a window
            imshow(img);
            % next add the image to the database
            %
                    if exist('img')
                        if (exist('face_database2.dat')==2)
```

```
                            load('face_database2.dat','-mat');
                            face_number=face_number+1;
                            data{face_number,1}=img(:);
                            prompt={strcat('Please Enter Your Customer No.
(Number must be a positive integer <= ',num2str(max_class), ')')};
                            title='Enter Customer No.';
                            lines=1;
                            def={'1'};
                            answer=inputdlg(prompt,title,lines,def);
                            zparameter=double(str2num(char(answer)));
                            if size(zparameter,1)~=0
                                class_number=zparameter(1);
                                if
(class_number<=0)||(class_number>max_class)||(floor(class_number)~=class_numb
er)||(~isa(class_number,'double'))||(any(any(imag(class_number))))
                                    warndlg(strcat('Class number must be a
positive integer <= ',num2str(max_class)),' Warning ')
                                else
                                    if class_number==max_class;
                                        max_class=class_number+1;
                                    end
                                    data{face_number,2}=class_number;

save('face_database2.dat','data','face_number','max_class','-append');
                                    msgbox(strcat('Database already exists:
image succesfully added to class number ',num2str(class_number)),'Database
result','help');
                                    close all;
                                    clear('img')
                                end
                            else
                                warndlg(strcat('Class number must be a
positive integer <= ',num2str(max_class)),' Warning ')
                            end
                        else
                            face_number=1;
                            max_class=1;
                            data{face_number,1}=img(:);
                            prompt={strcat(messaggio,'Class number must be a
positive integer <= ',num2str(max_class))};
                            title='Class number';
                            lines=1;
                            def={'1'};
                            answer=inputdlg(prompt,title,lines,def);
                            zparameter=double(str2num(char(answer)));
                            if size(zparameter,1)~=0
                                class_number=zparameter(1);
                                if
(class_number<=0)||(class_number>max_class)||(floor(class_number)~=class_numb
er)||(~isa(class_number,'double'))||(any(any(imag(class_number))))
                                    warndlg(strcat('Class number must be a
positive integer <= ',num2str(max_class)),' Warning ')
                                else
                                    max_class=2;
                                    data{face_number,2}=class_number;
                                    dimensioni = size(img);
```

```
save('face_database2.dat','data','face_number','max_class','dimensioni');
                                        msgbox(strcat('Database was empty.
Database has just been created. Image succesfully added to class number
',num2str(class_number)),'Database result','help');
                                        close all;
                                        clear('img')
                                    end
                                else
                                    warndlg(strcat('Class number must be a
positive integer <= ',num2str(max_class)),' Warning ')
                                end

                            end
                        else
                            errordlg('No image has been selected.','File Error');
                        end
    end
    if chos == 2

        clc;
        close all;
        if (exist('face_database2.dat')==2)
            button = questdlg('Do you really want to remove the Database?');
            if strcmp(button,'Yes')
                delete('face_database2.dat');
                msgbox('Database was succesfully removed from the current
directory.','Database removed','help');
            end
        else
            warndlg('Database is empty.',' Warning ')
        end
    end

    if chos==3,
        clc;
        close all;
        clear('img');
        if (exist('face_database2.dat')==2)
            load('face_database2.dat','-mat');
            msgbox(strcat('Database has ',num2str(face_number),' image(s).
There are',num2str(max_class-1),' class(es). Input images must have the same
size.'),'Database result','help');
        else
            msgbox('Database is empty.','Database result','help');
        end
    end

    if chos==4,
        clc;
        close all;
        helpwin facerecexplanation;
    end
    %----------------
    if chos==5,
        clc;
```

```
        close all;
        if (exist('face_database2.dat')==2)
            load('face_database2.dat','-mat');
            disp('Insert 0 to visualize total mean face');
            disp('Insert 1 to visualize class mean face');
            disp('Insert 2 to visualize the projection of input image onto
face-space');
            scelta = input('Insert your choice: ');
            if scelta == 0
                clc;
                matrice=zeros(size(data{1,1},1),face_number);
                for ii=1:face_number
                    matrice(:,ii)=double(data{ii,1});
                end
                somma=sum(matrice,2);
                media=somma/face_number;
                figure('Name','Total mean face');
                imshow(uint8(reshape(media,dimensioni)));
            end
            if scelta == 1
                clc;
                classescelta = input('Insert class number:');
                if classescelta <= max_class-1
                    somma     = zeros(size(data{1,1},1),1);
                    contatore = 0;
                    for ii=1:face_number
                        if data{ii,2}==classescelta
                            somma = somma + double(data{ii,1});
                            contatore = contatore+1;
                        end
                    end
                    somma = somma/contatore;
                    figure('Name','Class mean face');
                    imshow(uint8(reshape(somma,dimensioni)));
                else
                    warndlg('Class number is uncorrect',' Warning ');
                end
            end
            if scelta == 2
                clc;
                [namefile,pathname]=uigetfile('*.*','Select image');
                if namefile~=0
                    [img,map]=imread(strcat(pathname,namefile));
                    imshow(img);
                    dimensioni = size(img);
                else
                    warndlg('Input image must be selected.',' Warning ')
                end
                ingresso=double(img(:));
                % face_number is equal to "M" of Turk's paper
                % i.e. the number of faces present in the database.
                % These image are grouped into classes. Every class (or set)
should include
                % a number of images for each person, with some variations in
expression and in the
                % lighting.
                matrice=zeros(size(data{1,1},1),face_number);
```

```
                for ii=1:face_number
                    matrice(:,ii)=double(data{ii,1});
                end
                somma=sum(matrice,2);
                media=somma/face_number;
                for ii=1:face_number
                    matrice(:,ii)=matrice(:,ii)-media;
                end
                matrice=matrice/sqrt(face_number);
                % up to now matrix "matrice" is matrix "A" of Turk's paper
                elle=matrice'*matrice;
                % matrix "elle" is matrix "L" of Turk's paper

                % eigenvalues and eigenvectors of the "reduced" matrix  A'*A
                [V,D] = eig(elle);
                % the following multiplication is performed to obtain the
                % eigenvectors of the original matrix A*A' (see Turk's paper)
                % See also Karhunen-Loeve algorithm, for face recognition
                Vtrue=matrice*V*(abs(D))^-0.5;
                %Vtrue=matrice*V;
                Dtrue=diag(D);

                % the eigenvalues are sorted by order and only M' of them
                % are taken. We impose M' equal to the number of classes
                % (max_class-1)
                [Dtrue,ordine]=sort(Dtrue);
                Dtrue=flipud(Dtrue);
                ordine=flipud(ordine);
                Vtrue(:,1:face_number)=Vtrue(:,ordine);

                Vtrue=Vtrue(:,1:max_class-1);
                Dtrue=Dtrue(1:max_class-1);

                % we calculate the eigenface components of
                % the normalized input (mean-adjusted). I.e. the input
                % image is projected into "face-space"
                pesi=Vtrue'*(ingresso-media);


                figure('Name','Projection of inpu image onto face-space');
                imshow(uint8(reshape(Vtrue*pesi+media,dimensioni)))
            end
        else
            warndlg('Database is empty.',' Warning ');
        end
    end
    %----------------
end
```

MODIFIED PROGRAM TO VERIFY CUSTOMERS AT ATM COUNTER

```
%captosavepix.m
%this matlab program captures a cust image with a webcam and save it as
%into the face database
%
% first accept customer ID No (in terms of class, here)...
%
%prompt='Please Enter Your Customer ID No. :';
%title='Enter Customer ID';
%lines=1;
%def={''};
%answer=inputdlg(prompt,title,lines);
%custno=double(str2num(char(answer)));
%
clear;
clc;
chos=0;
possibility=2;
% set cropping values below
%crops = [horz1 vert1 horz2 vert2]
crops = [165 30 320 430]
messaggio='Insert the number of set: each set determins a class. This set
should include a number of images for each person, with some variations in
expression and in the lighting.';

while chos~=possibility,
    chos=menu('Fred Kayode ATM Face Authentication System','Validate
Customer','Exit');

    %----------------


    if chos == 1,
        % collect customer ID No (in terms of class, here)...
        prompt='Please Enter Your Customer ID No. :';
        title='Class number';
        lines=1;
        def={'1'};
        answer=inputdlg(prompt,title,lines,def);
        custno=double(str2num(char(answer)));
        % define video input object...to link matlab to the webcam
        f=videoinput('winvideo',2);
        %f=videoinput('winvideo',1);
        preview(f);
        waitfor(msgbox('Click OK to Capture Your Image for
Verification','Capture Image','help'));
        % snap an image shot with the video input object defined above...
        framex = getsnapshot(f);
        % close the preview window
        closepreview(f);
        imshow(framex)
        frame = imcrop(framex, crops)
```

```
         %frame = framex
         % display the acquired image in a window
        %imshow(frame);
        %imagesc(frame);
        %write the image into a pgm file and read back into another image
array
        imwrite(frame,'custpix.pgm');
        img = imread('custpix.pgm')
        imshow(img)    % display the pgm array...

        % Now go into the face recognition process

        if exist('img')
                    ingresso=double(img(:));
                    if (exist('face_database2.dat')==2)
                        load('face_database2.dat','-mat');
                        % face_number is equal to "M" of Turk's paper
                        % i.e. the number of faces present in the database.
                        % These image are grouped into classes. Every class
(or set) should include
                        % a number of images for each person, with some
variations in expression and in the
                        % lighting.
                        matrice=zeros(size(data{1,1},1),face_number);
                        for ii=1:face_number
                            matrice(:,ii)=double(data{ii,1});
                        end
                        somma=sum(matrice,2);
                        media=somma/face_number;
                        for ii=1:face_number
                            matrice(:,ii)=matrice(:,ii)-media;
                        end
                        matrice=matrice/sqrt(face_number);
                        % up to now matrix "matrice" is matrix "A" of Turk's
paper
                        elle=matrice'*matrice;
                        % matrix "elle" is matrix "L" of Turk's paper

                        % eigenvalues and eigenvectors of the "reduced"
matrix  A'*A
                        [V,D] = eig(elle);
                        % the following multiplication is performed to obtain
the
                        % eigenvectors of the original matrix A*A' (see
Turk's paper)
                        % See also Karhunen-Loeve algorithm, for face
recognition
                        if det(D)~=0
                            Vtrue=matrice*V*(abs(D))^-0.5;
                        else
                            Vtrue=matrice*V;
                        end
                        %Vtrue=matrice*V;
                        Dtrue=diag(D);
```

```
                        % the eigenvalues are sorted by order and only M' of
them
                        % are taken. We impose M' equal to the number of
classes
                        % (max_class-1)
                        [Dtrue,ordine]=sort(Dtrue);
                        Dtrue=flipud(Dtrue);
                        ordine=flipud(ordine);
                        Vtrue(:,1:face_number)=Vtrue(:,ordine);

                        Vtrue=Vtrue(:,1:max_class-1);
                        Dtrue=Dtrue(1:max_class-1);

                        % we calculate the eigenface components of
                        % the normalized input (mean-adjusted). I.e. the
input
                        % image is projected into "face-space"
                        [dd1, dd2] = size(media)
                        [ss1, ss2] = size(ingresso)
                        pesi=Vtrue'*(ingresso-media);

                        pesi_database          = zeros(max_class-1,max_class-
1);
                        pesi_database_mediati  = zeros(max_class-1,max_class-
1);

                        numero_elementi_classe=zeros(max_class-1,1);
                        for ii=1:face_number
                            ingresso_database=double(data{ii,1});
                            classe_database=data{ii,2};
                            pesi_correnti=Vtrue'*(ingresso_database-media);

pesi_database(:,classe_database)=pesi_database(:,classe_database)+pesi_corren
ti;

numero_elementi_classe(classe_database)=numero_elementi_classe(classe_databas
e)+1;
                        end
                        for ii=1:(max_class-1)

pesi_database_mediati(:,ii)=pesi_database(:,ii)/numero_elementi_classe(ii);
                        end
                        % pesi_database_mediati is a matrix with the averaged
eigenface components of the images
                        % present in database. Each class has its averaged
eigenface.
                        % We want to find the nearest (in norm) vector to the
input
                        % eigenface components.

                        distanze_pesi=zeros(max_class-1,1);
                        for ii=1:(max_class-1)
                            % distanze_pesi(ii)=norm(pesi-
pesi_database_mediati(:,ii));
                            distanze_pesi(ii) = sum((abs(pesi-
pesi_database_mediati(:,ii))));
```

```
                        end


[minimo_pesi,posizione_minimo_pesi]=min(distanze_pesi);

                        % now we are evaluating the distance of the mean-
normalized
                        % input face from the "space-face" in order to
detrmine if
                        % the input image is a face or not.
                        proiezione=zeros(size(data{1,1},1),1);
                        for ii=1:(max_class-1)
                            proiezione=proiezione+pesi(ii)*Vtrue(:,ii);
                        end
                        distanza_spazio_facce=norm((ingresso-media)-
proiezione);


                        messaggio1='See Matlab Command Window to see matching
result. The program has just calculated the minimal distance from classes and
the distance from Face Space. ';
                        messaggio2='You now should fix the two threshold-
values to determine if this mathing is correct. If both distances are below
the threshold values it means that the input ';
                        messaggio3='face was correctly matched with a known
face. If the distance from Face Space is below the threshold value but the
minimal distance from classes is above the other threshold value, ';
                        messaggio4=' it means that the input image is an
unknown face. See the cited article for more informations.';


%msgbox(strcat(messaggio1,messaggio2,messaggio3,messaggio4),'Matching
result','help');

                        % NOW DISPLAY THE RESULT OF THE FACE RECOGNITION...


                        thresh_class=23700
                        thresh_dist4mfacespc=23500
                        if custno == posizione_minimo_pesi
                            if (minimo_pesi < thresh_class &
distanza_spazio_facce < thresh_dist4mfacespc)
                                msg1 = 'You have been succesfully
authenticated : You are the true owner of this account'
                                msgbox(msg1,'Face recognition
Result','help');
                            else
                                msg1 = 'Authentication failed : You are not
the owner of this account'
                                msgbox(msg1,'Face recognition
Result','help');
                            end;
                        else
                            msg1 = 'Authentication failed : You are not the
owner of this account'
```

```
                            msgbox(msg1,'Face recognition Result','help');
                        end

                        mesg1='The nearest class is number  ';
                        mesg2 =strcat(num2str(posizione_minimo_pesi),'; \n');
                        mesg3='with a distance equal to  ';
                        mesg4 =strcat(num2str(minimo_pesi), '; \n');
                        mesg5 = 'The distance from Face Space is  ';
                        mesg6=num2str(distanza_spazio_facce);

msgbox(strcat(mesg1,mesg2,mesg3,mesg4,mesg5,mesg6),'Face recognition
Result','help');

                        %disp('The nearest class is number ');
                        %disp(posizione_minimo_pesi);
                        %disp('with a distance equal to ');
                        %disp(minimo_pesi);
                        %disp('The distance from Face Space is ');
                        %disp(distanza_spazio_facce);

                    else
                        warndlg('No image processing is possible. Database is
empty.',' Warning ')
                    end
                else
                    warndlg('Input image must be selected.',' Warning ')
        end


        clc;
        close all;
    end

end
```