بسم الله الرحمن الرحيم

ألم نجعل له عينين 8

ولسانا وشفتين 9

وهديناه النجدين 10

صدق الله العظيم

# ACCESS WINDOWS BY IRIS RECOGNITION

This thesis is presented to the Graduate School
In fulfilment of the requirements for
Master of Science (Information Technology)
University Utara Malaysia

By

**Musab A. M. Ali**

# PERMISSION TO USE

In presenting this thesis of the requirements for a Master of Science in Information Technology (MSc. IT) from Universiti Utara Malaysia, I agree that the University library may make it freely available for inspection. I further agree that permission for copying of this project in any manner, in whole or in part, for scholarly purposes may be granted by my supervisor or in their absence, by the Dean of College of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my project.

Request for permission to copy or make other use of materials in this project, in whole or in part, should be addressed to:

Dean of College of Arts and Sciences
Universiti Utara Malaysia
06010 Sintok
Kedah Darul Aman

# ACKNOWLEDGEMENTS


*All the praises and thanks are to Allah, the Lord of the 'Alamin'*

First, I would like to express my gratitude to my supervisor, Associate Professor Fadzilah Siraj and Madam Nur Azzah Abu Bakar for expertise, gentle guidance and encouragement, which ensured that, progress was continuously maintained. Our discussions since the last three months have contributed to the completion of this work.

I also would like to express my thanks to the University Utara Malaysia, especially to my colleagues of the Faculty of Information Technology, for the enjoyable working environment, and for the given support. I owe particular thanks to the people that contributed for the earliest stage of this work, by offering themselves as volunteers, in the construction of the UBIRIS database.

Last, but not least, I would like to thank my parents for their endless encouragement, my brother Ammar, my sisters and all the people close to myself, for their strong support, encouragement, friendship and love. I am grateful for their understanding during the time during which I was absent due to this project work.

Sincere Grateful

***Eng. Musab A. M. Ali***

# ABSTRACT

*This project aims to design and develop an iris recognition system for accessing Microsoft Windows. The system is built using digital camera and Pentium 4 with SVGA display adapter. MATLAB ver. 7.0 is used to preprocess the taken images convert the images into code and compare the picture code with the stored database. The project involves two main steps: (1) applying image processing techniques on the picture of an eye for data acquisition. (2) applying Neural Networks techniques for identification .The image processing techniques display the steps for getting a very clear iris image necessary for extracting data from the acquisition of eye image in standard lighting and focusing. In a use of your images, the images are enhanced and segmented into 100 parts. The standard deviation is computed for every part in which the values are used for identification using NN techniques. Locating the iris is done by following the darkness density of the pupil. For all networks, the weights and output values are stored in a text file to be used later in identification. The Backprobagation network succeeded in identification and getting best results because it attained to (False Acceptance Rate = 10% - False Rejection Rate = 10%), while the Linear Associative Memory network attained to (False Acceptance Rate = 20% - False Rejection Rate = 20%)*

# TABLE OF CONTENTS

# TABLE OF FIGURE

# TABLE OF TABLE

# CHAPTER ONE

# INTRODUCTION

Biometrics is a study of methods for recognizing and identifying a person based upon one or more intrinsic physical or behavioral traits such as fingerprints, Deoxy Ribonucleic Acid (DNA) or retinal patterns (Russ, 2004). A good biometric identifier has two basic characteristics: [1] stability [2] distinctiveness. A stable biometric does not change over time thus hair length would not be a good identifier. Meanwhile a distinctive biometric is unique to an individual (Mohammed *et al.,* 2004).

Traditionally, personal identification is based upon what a person possesses for example a physical key or identity (ID) card. It can also base upon what a person knows, e.g. a password. However these methods have some limitations: keys and ID cards may be lost or misplaced while passwords may be forgotten. Biometrics, on the other hand, minimizes those risks as it uses traits that are part of humans. In recent years, biometric personal identification grows as an interesting field from industrial and academic point of view (Zhu *et al.,* 2000). It provides an alternative to username and password, as well as to smart card. Biometrics seeks to tie identity much more tightly to a person's particular unique features. These could be anatomical, physiological, or even behavioral. The sounds of a person's voice, or they way in which they sign their name, are examples of behavioral biometrics. Their blood type or markers in their tissue or fluid samples (including DNA itself) are examples of physiological biometrics which are typically used in forensic applications. Most currently used biometrics is anatomical, i.e. facial appearance, hand geometry, fingerprints, retinal vein patterns, and iris patterns (Amer, 2001). Biometrics has been around since (1980), yet it is only recently that it has started to gain foothold within the computing and communication industry for consumer applications (Zhang, 2000).

Essentially, all biometric systems operate in the same fashion. First, it captures a sample of the biometric characteristic; then unique features are extracted and converted into mathematical code. Depending upon the needs and technology, several samples could be taken to build the confidence level of the initial data. These data are stored as biometric templates for a particular person. When identity needs to be checked, features from a person are extracted and compared with the stored information for validation (Lawton, 1998). One of the most mathematically unique biometric is the iris of the eye. Figure 1.1 below shows the iris that surrounds the pupil, and is located behind the cornea of the eye and the aqueous humor, but in front of the lens. Its purpose is to control the amount of light that enters the eye through the pupil, by the action of its dilator and sphyncter muscles that control pupil size, but its construction from elastic connective tissue gives it a complex, fibrillose pattern.

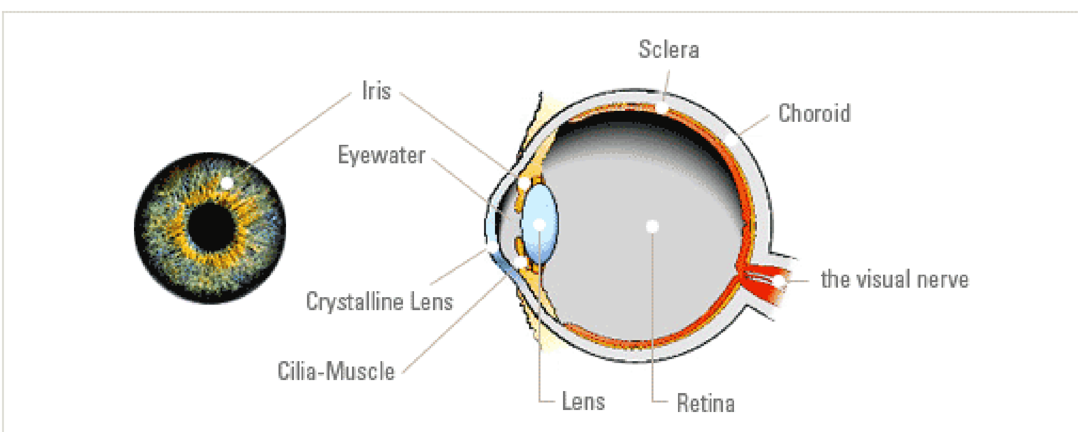



**Figure 1.1:** The eye parts

Human iris is absolutely unique, even between twins or an individual's right and left eyes. The iris itself is stable throughout a person's life, approximately from the age of one. Unlike other biometric traits, such as fingerprints, facial, retina and voice, the physical characteristics of the iris do not change with age. Due to this, iris recognition technology can provide higher level of accuracy and speed in preprocessing the input data, as well as more cost-effective compared to fingerprint, facial, retina and voice (Roizenblatt *et al*., 2004). Iris recognition system combines computer vision, pattern recognition, statistics, and the human-machine interface. The purpose is real-time, high confidence recognition of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. Because the iris is a protected internal organ whose random texture is stable throughout life, it can serve as a kind of living passport or a living password that one need not remember but one always carries along (Rosenzweig *et al*., 2004). The system controls access to assets that require unique identification and/or verification of individuals. For example, iris recognition can be applied at a doorway so that only authorized individuals can gain access through it.

Currently, most iris recognition systems are used to control access to assets that require very high security levels, such as buildings or office spaces that contain highly sensitive material or classified information. Other applications that are currently using iris recognition include security applications at border crossings and passenger screening for frequent flyers at airports (Patina, 2003). The system works by capturing a high resolution digital photograph of the individual's iris. The unique features contained in the iris are compared against a database so that the identity of the individual can be determined. Iris technology is non-intrusive as a person does not need to touch anything to use the system. Automatic voice prompting, auto focus, plus enrollment and recognition speed make the system easy to use. An individual is detected automatically upon approaching the imager, i.e. the digital camera. A glances at the aperture mirror from 3-10" distance allows the camera to capture an iris image, which is digitally processed into a 512 byte Iris Code® record.

## 1.1 Problem Statement

The use of physical files and cabinets for storing information has been replaced by computers; this allows organizations and individuals to store such valuable assets in digital forms. Despite easy to retrieve and transfer, digital information is more vulnerable to hackers and spongers (Grossman, 2008). This raises a need to improve security of such information by limiting access only to those who have authorization to do so. The traditional means, as well as biometric traits other than iris, do provide such control; yet they still have several limitations in verifying the identity of individuals.

## 1.2 Research questions

This project aims to answer the following research questions:

(a) How to identify system requirements that are related to iris recognition?

(b) How to develop and test a neural network model used in iris recognition?

## 1.3 Research objectives

This project aims to improve the security of information being stored in computers by controlling access to it. The objectives of this project, therefore, are as follows:

(a) To identify recognition system requirements that are related to iris recognition

(b) To develop and test the neural network model used in iris recognition prototype

**1. 4 Scope of the project**

This project develops an iris recognition system to improve the security of digital information being stored in either desktops or laptops running on Microsoft Windows operating system. It uses only one biometric feature, i.e. the iris, as a means to verify the identity of a person before granting access to the information. A high resolution digital camera is used to capture the image; once captured, the iris portion of the image is isolated and transformed into templates. The patterns are matched with those registered in the database in which access is granted to individuals only when a match is found.

**1.5 Significance of the project**

The major contribution of this project is an iris recognition system for controlling access to Windows, which should be viewed as the first step towards developing a larger scale security system based upon biometric features of humans. It contributes to the body of knowledge in that it provides evidence of the usefulness of using iris for verifying the identity of individuals; in other words it proves that iris is reliable.

**1.6 Organization of the report**

This report is organized into five chapters. Chapter 1 is an introduction chapter that explains the background overview, problem statements, research questions and objectives, as well as scope and significance of the project. State-of-the-arts of the related issues are discussed in Chapter 2. Chapter 3 describes the methodology used in this study. The result of the study and the conclusion are discussed in Chapter 4 and Chapter 5 respectively.

# CHAPTER TWO

# LITERATURE OVERVIEW

The ever increasing use of computers and the Internet as tools of information technology brought with it the necessity to protect personal or commercial information from unauthorized access by individuals or companies. As many organizations and individuals use computers as places to store their confidential information, security of this place has become one of the central issues in computing, For example, the Manger International Nevada (MIN) company entered into a computer to traffic manager and the theft of their contents and said the company

Bankruptcy, Or robbing a bank when he entered a computer staff to the Director and transferred to the account abroad million dollar (Tom, 2004).

People have long been using keys, identity cards, smart cards, passwords as well as biometrics to prevent unauthorized access to secured places. Biometrics involves use of physical and behavioral traits of humans which include fingerprint (Omlin *et al.,* 2000), Deoxy Ribonucleic Acid (DNA) (Aminzadeh *et al.,* 2000), retinal patterns (Chang *et al.,* 2000), voice (Chen *et al.,* 1993), handwriting (Berry *et al.,* 1997), iris (Wong *et al.,* 1995) and others. These traits have several advantages over keys, IDs and passwords; as they are part of humans, biometrics will never be misplaced or forgotten. Besides, they are more reliable due to the fact that they are unique to individuals

Sections 2.1 to 2.2 of this chapter present an overview of biometric technology, and biometric applications in information security. Section 2.4 describes a specific biometric feature that becomes the focus of this study, i.e. the iris. The iris recognition technology is described, as well as its applications in various application domains. The information security issues are discussed in Section 2.8. The use of Neural Networks in iris recognition systems.

## 2.1 Overview of biometric technology

Biometrics refers to a unique, measurable characteristic or trait of a human being for recognizing or verifying the identity of individuals. The term biometrics is derived from the Greek words "bios", which means *life*, and "metron", which means *measure*. Biometrics also refers to an entirely different field (today more commonly called

Biostatistics), which concerns about the development of statistical and mathematical methods applicable to data analysis problems in the biological sciences (Zhang, 2000).

There are two major categories of biometric features: [1] physiological and [2] behavioral. Physiological biometric identification measures unique body characteristics such as fingerprint details, retina blood vessel patterns, features of iris, the size and shape of hand or facial scan. It compares these characteristics against a pattern recorded during an enrollment process. Behavioral measurement, on the other hand, identifies unique learned traits such as person's signature, voice scan and keystrokes scan (Wildes *et al*., 1996). The degree of intra-personal variation in a physical characteristic is smaller than a behavioral characteristic. For example, a signature is influenced by both controllable actions and less psychological factors, while speech pattern on the other hand is influenced by current emotional state

Biometrics technology is becoming increasingly popular due to several reasons (Daugman, 1993). First, it provides convenient authentication. With biometric technology, there is nothing to loose or forget since the characteristics or traits of the person serve as the identifiers. Many of these "individual" identifiers remain relatively unchanged and are enduring over time. In addition, biometric technologies also provide greater convenience for the information technology and support organizations that manage user authentication. For example, biometrics helps to eliminate the need to replace badges or reset personal identification numbers. The second reason is because there is an increasing need for strong authentication. Biometrics should reduce the risk of compromising the likelihood that an adversary can present a suitable identifier and gain unauthorized access. With today's intense focus on greater security for logical computer and physical access, biometrics offers an attractive method for guarding against stolen or lost identifiers, such as cards or passwords. The improvement in hardware and software technologies has become another reason why the technology becomes popular. Such improvement has brought down the costs of biometric authentication to be suitable at the commercial market level. The various types of biometric technology are as described in section 2.1.1 to 2.1.6 below.

### 2.1.1 Fingerprint Recognition

Fingerprint recognition technology is probably the most widely used and well-known biometric. Fingerprint recognition relies on features found in the impressions made by distinct ridges on the fingertips. The two types of fingerprints are flat and rolled in which flat prints is an impression of only the central area of the finger pad, while rolled prints capture ridges on the sides of the finger as well as the central portion between the tip and first knuckle. Fingerprint images are scanned, enhanced and then converted into templates. These templates are saved in a database for future comparisons using optical, silicon or ultrasound scanners. Optical scanners are the most commonly used despite the fact that ultrasound scanners can produce the most accurate results (Rosenzweig *et al*., 2004).

### 2.1.2 Facial Recognition

Face recognition technology identifies individuals by analyzing certain facial features such as the upper outlines of the eye sockets or sides of the mouth. Typically, facial recognition compares a living person with a stored template, but it has also been used for comparison between static images and templates. This technology is a biometric system that can routinely be used in a secure manner, for surveillance, since a person's face is easily captured by video technology (Rosenzweig *et al*., 2004).

### 2.1.3 Voice recognition

Voice recognition technology for identifying people is based on the differences in the voice resulting from learned speaking habits. When an individual is enrolled, the system captures samples of the person's speech as the individual says certain scripted information into a microphone or telephone multiple times. This information is known as a pass phrase, which is then converted into a digital format. The distinctive characteristics (e.g. pitch, cadence and tone) are extracted to create a template for the speaker. Voice recognition templates require the most data space of all the biometric templates (Wildes *et al*., 1996). The accuracy of voice recognition, however, can be affected by behavioral characteristic which can negatively be affected by the current physical condition and the emotional state. The background and noise in the input signal is another influencing factor which increases the false rejection rate (Riha *et al*., 2000).

### 2.1.4 Retina scan

Retina scan is based on the blood vessel pattern in the retina of the eye. Retina scan technology is older than the iris scan technology that also uses part of the eye. The major drawback of retina scan is its intrusiveness; the method of obtaining a retina scan is personally invasive as a laser light must be directed through the cornea of the eye. It is also noted in Riha *et al*., (2000) that the operation of the retina scanner is not easy.

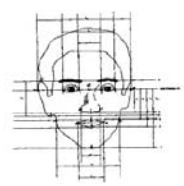
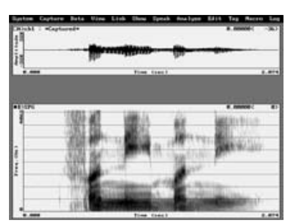
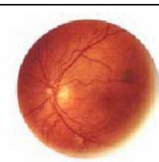
### 2.1.5 Hand geometry

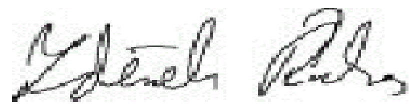
Hand geometry is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after a certain age. Hand geometry systems produce an estimation of certain measurements of the hand such as the length and the width of fingers. Various methods are used to measure the hand; the optical method is much more common today. Optical hand geometry scanners capture the image of the hand and use the image edge detection algorithm to compute the hand's characteristics. Only two-dimensional (2D) characteristics of the hand can be used in this case (Riha *et al*., 2000).

### 2.1.6 Signature dynamics

The signature dynamics recognition is based on the dynamics of making the signature, rather than a direct comparison of the signature itself afterwards. The dynamics is measured as a means of the pressure, direction, acceleration and the length of the strokes, number of strokes and their duration. Pioneers of the signature verification first developed a reliable statistical method in 1970s. This involved the extraction of ten or more writing characteristics such as the number of times the pen was lifted, the total writing time and the timing of turning points (Dory *et al*., 2001). Table 2.1 below shows pictures of the biometrics that have been mentioned above.

**Table 2.1:** Biometric pictures

| **Biometrics** | **Pictures** |
|---|---|
| **Fingerprint** |  |
| **Facial** |  |
| **Voice** |  |
| **Retina** |  |

| | |
|---|---|
| **Hand geometry** |  |
| **Signature dynamics** |  |

Besides, newer biometrics technology include other human traits such as DNA, ear shape, odor, vein scan, fingernail bed, gait, palm print and keystroke. A brief description of each of these newer biometric technologies is as in Table 2.2.

**Table 2.2:** New biometric technologies

| Biometric | Description |
|---|---|
| **Palmprint** | Palmprint verification is a slightly different implementation of the fingerprint technology. Palmprint scanning uses optical readers that are very similar to those used for fingerprint scanning; their size is much bigger which is limiting factor for the use in workstations or mobile devices. |
| **Hand vein** | Hand vein geometry is based on the fact that the vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera. The hand vein geometry is still under the stage of research and development.<br>Hand vein map led to a new similar technology called "Thermal Imaging". It also uses an infrared source of light and camera to |

| | |
|---|---|
| | produce an image of the vein pattern in the face or in the wrist. |
| **DNA** | DNA sampling is rather intrusive at present and requires a form of tissue, blood or other bodily sample. This method of capture still has to be refined. So far, the DNA analysis has not been sufficiently automatic to rank the DNA analysis as a biometric technology. As soon as the technology advances so that DNA can be matched automatically in real time, it may become more significant. At present, DNA is very entrenched in crime detection and so will remain in the law enforcement area for the time being. |
| **Ear shape** | Identifying individuals by the ear shape is used in law enforcement applications where ear markings are found at crime scenes. Whether this technology will progress to access control applications is yet to be seen. An ear shape verifier (Otophone) is produced by a French company ART Techniques. It is a telephone type handset within which is a lighting unit and cameras which capture two images of the ear. |
| **Keystroke** | Keystroke dynamics is a method of verifying the identity of an individual by their typing rhythm which can cope with trained typists as well as the amateur two-finger typist. Systems can verify the user at the log-on stage or they can continually monitor the typist. |
| **Fingernail bed** | The US Company AIMS is developing a system which scans the dermal structure under the fingernail. This tongue and groove |

| | |
|---|---|
| | structure is made up of nearly parallel rows of vascular rich skin. Between these parallel dermal structures are narrow channels and it is the distance between these which is measured by the AIMS system (Daugman, 1993). |

Mean will Figure below shows all approaches to protect information security.

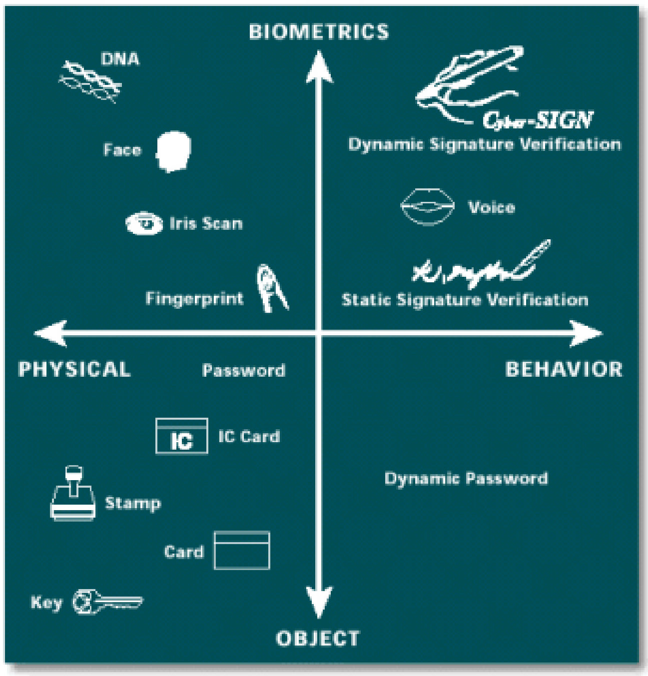



**Figure 2.1:** The biometric system security

## 2.2 Comparison of various biometric technologies

It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters (Jain, 2004):

1. Universality describes how commonly a biometric is found individually.
2. Uniqueness is how well the biometric separates individually from another.
3. Permanence measures how well a biometric resists aging. Collectability eases of acquisition for measurement.

4. Collectability eases of acquisition for measurement.

5. Performance accuracy, speed, and robustness of technology used. Acceptability degree of approval of a technology.

6. Acceptability degree of approval of a technology.

7. Circumvention eases of use of a substitute.

The following table shows as a comparison between the existing biometric systems in terms of the above parameters, which are represented by the numbers 1 to 7. The letters H, M and L mean high, medium and low ranking respectively.

**Table 2.3:** Comparison of various biometric technologies, according to (Jain, 2004).

| Biometrics: | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| Face | H | L | M | H | L | H | L |
| Fingerprint | M | H | H | M | H | M | H |
| Hand geometry | M | M | M | H | M | M | M |
| Keystrokes | L | L | L | M | L | M | M |
| Hand veins | M | M | M | M | M | M | H |
| Iris | H | H | H | M | H | L | H |
| Retinal scan | H | H | M | L | H | L | H |
| Signature | L | L | L | H | L | H | L |
| Voice | M | L | L | M | L | H | L |
| facial thermograph | H | H | L | H | M | H | H |
| Odor | H | H | H | L | L | M | L |
| DNA | H | H | H | L | H | L | L |
| Gait | M | L | L | H | L | H | M |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Ear recognition** | M | M | H | M | M | H | M |

Jain (2004) ranks each biometric based on the categories as being low, medium, or high. A low ranking indicates poor performance in the evaluation criterion whereas a high ranking indicates a very good performance. Another comparison, which is based of the characteristics, is as shown in Table 2.4

**Table 2.4:** Comparison of biometric systems based on their characteristics

| Characteristic | Fingerprints | Hand geometry | Retina | Iris | Face | Signature | Voice |
|---|---|---|---|---|---|---|---|
| **Ease of Use** | High | High | Low | Medium | Medium | High | High |
| **Error incidence** | Dryness, dirt, age | Hand injury, age | Glasses | Poor Lighting | Lighting, age, glasses, hair | Changing signatures | Noise, colds, weather |
| **Accuracy** | High | High | Very High | Very High | High | High | High |
| **User acceptance** | Medium | Medium | Medium | Medium | Medium | Medium | High |
| **Required security level** | High | Medium | High | Very High | Medium | Medium | Medium |
| **Long-term** | High | Medium | High | High | Medium | Medium | Medium |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **stable** | | | | | | | |

Al-Sumaidaee (2005), on the other hand, compares between the various biometric systems in terms of cost versus accuracy, as shown in Figure 2.2. The physiological biometrics systems are shown to be more accurate and more costly than the behavioral biometrics systems (Mohammed *et al.,* 2004). In light of this, it can be concluded that when the cost and accuracy of the technology increased, the level of security it can provide is also increased.

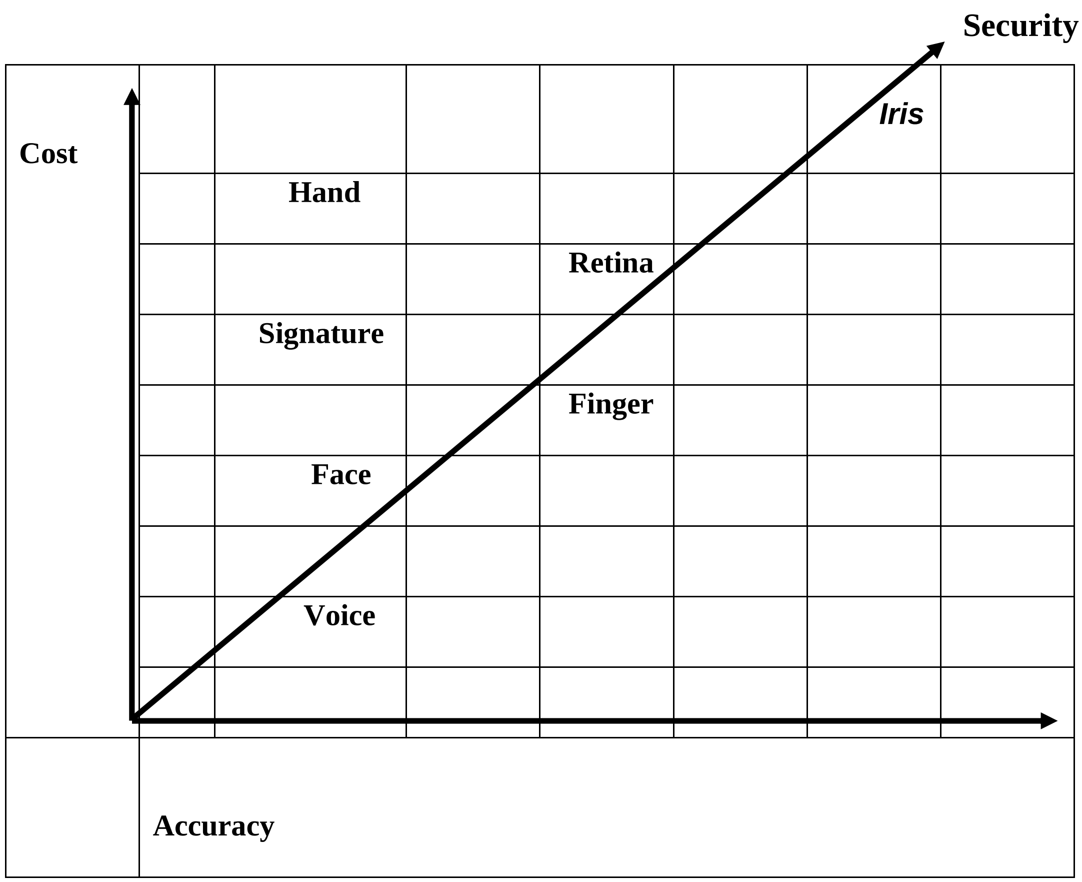



**Figure 2.2:** Cost versus accuracy and security for different biometric systems

**2.3 Biometric Applications**

The various apprications of biometrics are described in (Fornell *et al.*, 2004; Garbarino *et al.,* 1999; Grossman *et al.,* 2008; Hand *et al.,* 2001; Hastie *et al.,* 2001; Hruschka *et al.,* 2001; Johnson, 1991; Kukula *et al.,* 2005; Wayman, 2006; Ammar 2005; John, 2005, Wilson *et al.*, 2003, Bajer, 2005 and Reynolds, 2004). Among the applications are facial scanning used to recognize employees at the in international airports (Fornell *et al.,* 2004); facial scanning used to recognize known criminals before they enter a different country (Garbarino *et al.,* 1999); fingerprint scanning used in federal and local government agencies to identify employees and prisoners (Grossman *et al.,* 2008); iris scanning for identification and verification of customers at the bank's ATM (Hand *et al.,* 2001); iris scanning for highly sensitive restrictive areas that is used by government and in military sites (Hastie *et al.,* 2001); voice recognition used in financial institutions, corporations, and government agencies in their telephony applications (Hruschka *et al.*, 2001); as well as fingerprint used by individuals to prevent unauthorized uses of their credit cards (Johnson, 1991).

In addition to the above, iris recognition is used in Brazil and most South American countries for personal identification (Kukula *et al.*, 2005). Wayman (2006) describes iris recognition used by the United States government. Yet, privacy activists in many countries have criticized the use of the technology for the potential harm to civil liberties, privacy, and the risk of identity theft. Currently, there is some apprehension in the United States (and the European Union) that the information can be "skimmed" and identify people's citizenship remotely for criminal intent, such as kidnapping. There also are technical difficulties currently delaying biometric integration into passports in the United States, the United Kingdom, and the rest of the EU. These difficulties include compatibility of reading devices, information formatting, and nature of content (e.g. the US currently expect to use only image data, whereas the EU intends to use fingerprint and image data in their passport RFID biometric chips).

Meanwhile, in Germany, the biometrics market is expected to experience enormous growth with the market size increases from approximately 12 million euro in 2004 to 377 million euro in 2009 (Ammar, 2005). According to Eva (2005) the federal government will be a major contributor to this development. In particular, the biometric procedures of fingerprint and facial recognition can profit from the government project (Hocquet *et al.,* 2005). In May 2005 the German Upper House of Parliament approved the implementation of the E-Pass, a passport issued to all German citizens that contains biometric technology. The E-Pass has been in circulation since November 2005.

Initially, the chip only held a digital photo of the holder's face; starting from March 2007, fingerprints were also stored on the chips (Reynolds, 2004). An increase in the prevalence of biometric technology in Germany is an effort to not only keep citizens safe within German borders but also to comply with the current US deadline for visa-waiver countries to introduce biometric passports ( Philips *et al.,* 2005).

Visitors intending to visit Australia may soon have to submit to biometric authentication as part of the Smartgate system, linking individuals to their visas and passports (Wilson *et al*., 2003). Biometric data are already collected from some visa applicants by the Department of Immigration and Citizenship Australia. Other applications include authentication of gym users. Biometrics has been used extensively in Israel for several years (Bajer, 2005). The border crossing points from

Israel to the Gaza Strip and West Bank are controlled by gates through which authorized Palestinians may pass. Thousands of Palestinians pass through the turnstiles every day to work in Israel, and each of them has an ID card which has been issued by the Israeli Military at the registration centers. The ID card is a smartcard with stored biometrics of fingerprints, facial geometry and hand geometry. In addition there is a photograph printed on the card and a digital version stored on the smartcard chip. The Tel Aviv Ben Gurion Airport has a frequent flyer's fast check-in system which is based on the use of a smartcard which holds information relating to the holders hand geometry and fingerprints. For a traveller to pass through the fast path using the smartcard system takes less than 10 seconds. The Immigration Police at Tel Aviv Airport use a system of registration for foreign workers that utilize fingerprint, photograph and facial geometry which are stored against the Passport details of the individual. There is a mobile version of this which allows the police to check on an individual's credentials at any time.

Biometrics is being used extensively in Iraq to catalogue as many Iraqis as possible providing Iraqis with a verifiable identification card, immune to forgery. (Reynolds, 2004) During account creation, the collected biometrics information is logged into a central database which then allows a user profile to be created. Even if an Iraqi has lost their ID card, their identification can be found and verified by using their unique biometric information. Additional information can also be added to each account record, such as individual personal history. This can help American forces determine whether someone has been causing trouble in the past. One major system in use in Iraq is called BISA (John, 2003). This system uses a smartcard and a user's fingerprint, iris, and face photos to ensure they have authorized access to a base or facility.

Several banks in Japan have adopted palm vein authentication technology on their ATMs. This technology which was developed by Fujitsu, among other companies, proved to have low false rejection rate (around 0.01%) and a very low false acceptance rate (less than 0.00008%) (Reynolds, 2004).

## 2.4 Iris Recognition

Iris is a colored circular muscle, which is beautifully pigmented giving us our eye's color (the central aperture of the iris is the pupil). This circular muscle controls the size of the pupil so that more or less light, depending on illumination conditions, is allowed to enter the eye (Mohammed *et al.,* 2004).

Figure 2.3 shows the iris features that consist of lines, dots, rings, rifts, pits, crypts, freckles, striations, contraction furrows, coronas and serpentine vasculature (Mohammed *et al*., 2004; Dory *et al*., 2001; Daugman, 1993). Scientists have identified 250 features unique to each person's iris, compared to about 40 for fingerprints. It remains constant through a person's life, unlike a voice or a face, fingerprint and hand patterns which can be changed through alteration or injury. In light of this, Mohammed *et al.,* (2004) claimed that iris identification is more accurate than the other high-techniques identification systems available that scans voices, faces, and fingerprints

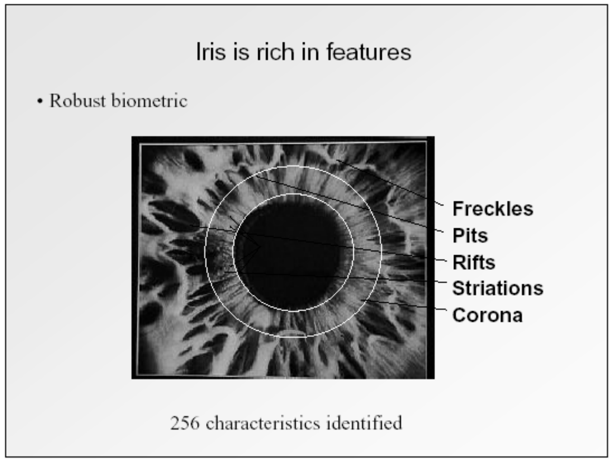



**Figure 2.3:** Iris features

Iris is the most individually distinctive feature of the human body. No two irises are alike, not even among twins (Mohammed *et al*., 2004; Nam *et al*., 2004). In fact, left and right irises of one individual are not identical. The statistical probability that two irises are never being exactly the same is estimated at 1 in $10^{72}$. Therefore, iris recognition is statistically more accurate than DNA testing (Burghardt, 2002). In light of this iris patterns provides an alternative approach to reliable visual recognition of persons when imaging can be done at distances of less than a meter, and especially when there is a need to search very large databases without incurring any false matches despite a huge number of possibilities. Although small, i.e. in 11mm size, and sometimes problematic to image, the iris has the great mathematical advantage that its pattern variability among different persons is enormous. Iris colour is determined mainly by the density of melanin pigmint in its anterior layer and stroma, with blue irises resulting from an absence of pigment long-wavelength light penetrates while shorter wavelengths are scattered by the stroma (Daugman, 2004).

However, the iris pattern is highly detailed in that the identification procedure becomes more difficult.

Because of its reliability and ease of use, iris recognition technology is gaining popularity across the globe in areas such as public safety, aviation, education and health care (Dory *et al.*, 1999). Among the examples are those used in large and small county correctional systems across the United States (Zhu *et al.*, 2000), as well as at the Charlotte Airport in North Carolina and the Flughafen Frankfort Airport in Germany to streamline boarding procedures (Roizenblatt *et al*., 2004). There is discussion that banks may someday make iris scans a routine part of ATM transactions and some have begun taking the first steps in testing out these systems (Roizenblatt *et al*., 2004). Others include those used in hospitals in Washington, D.C., Pennsylvania and Alabama; infant nursing stations in Germany; school in New Jersey and voluntary repatriation centers in Pakistan (Roizenblatt *et al.*, 2004; Patina, 2003).

### 2.4.1 Iris recognition algorithms

The idea of using iris patterns for personal identification was originally proposed b y an ophthalmologist named Frank Burch in 1936. In the 1980's the idea had appeared in fictions cinema films, but it still remained as a science fiction and conjecture. In 1981, after reading many scientific reports describing the iris great variation, Flom (2007) and San Francisco's ophthalmologist Aran Safir (2006) also suggested the use of the iris as the basis for a biometric. In 1987, they began collaborating with computer scientist John Daugman of Cambridge University in England, who published his first promising results in 1992, to develop iris identification software (Burghardt, 2000).

### 2.4.2 Iris recognition step

Figure 2.4 below shows the steps involved in iris recognition process, as described in Smith (1999).

Step 1: Start program for iris recognition system.

Step 2: Take a picture of face and cut their eye and from camera height accuracy.

Step 3: Processing techniques on the iris image from eye.

Step 4: convert the iris to code in data accommodation.

Step 5: processing neural network (Backprobagation) use the code for iris.

Step 6: check if the new user add/ storage in data base or comparing iris pattern with database storage.

Step 7: Recognizing signal end or return.

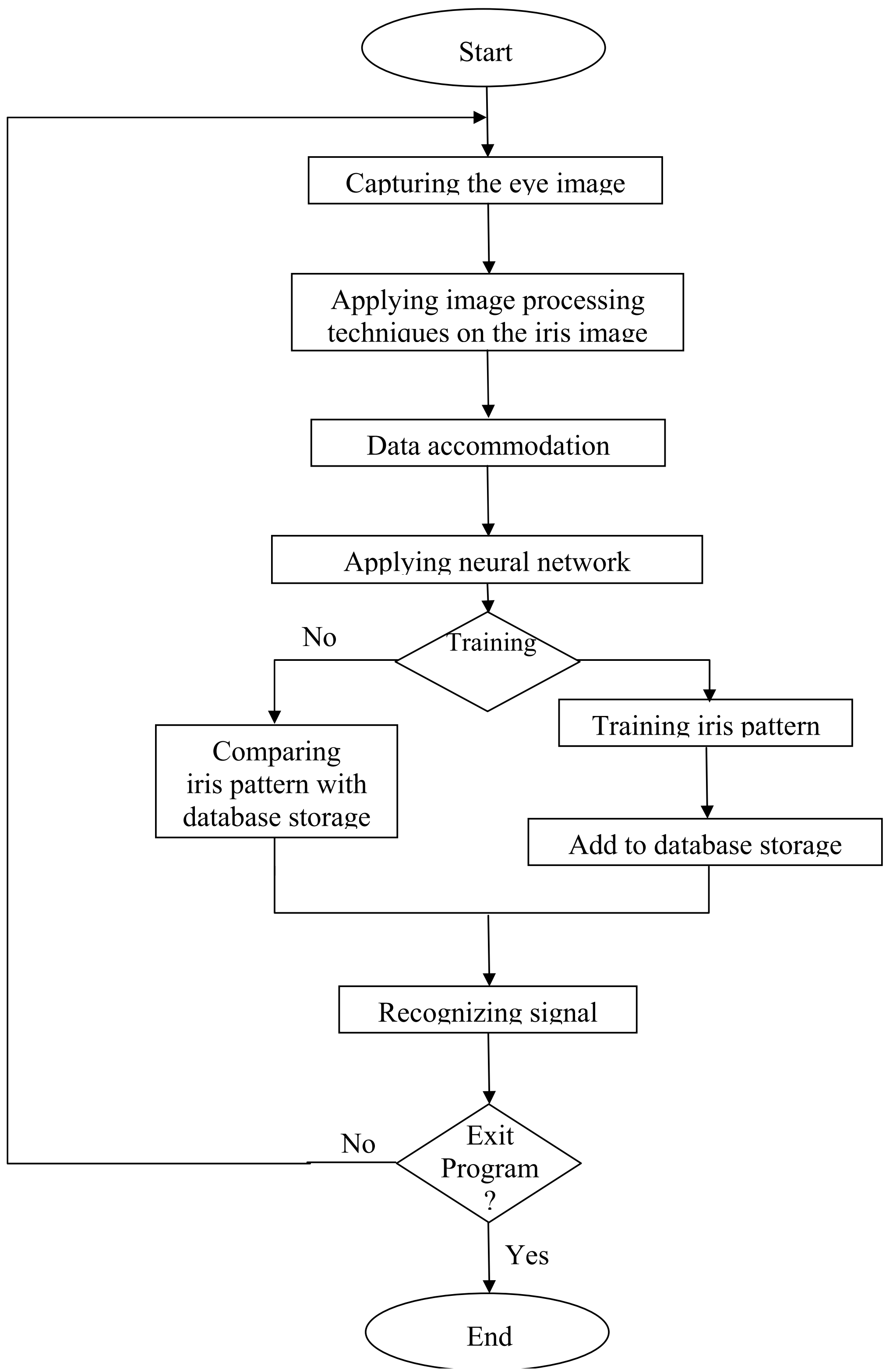



**Figure 2.4:** Iris recognition steps

**2.5 Information secu**

This section reviews some existing information security system for widow's access. NSA access was built into Windows Careless mistake reveals subversion of Windows by NSA. A CARELESS mistake by Microsoft programmers has revealed that special access codes prepared by the US National Security Agency have been secretly built into Windows. The NSA access system is built into every version of the Windows operating system now in use, except early releases of Windows 95 (and its predecessors). The discovery comes close on the heels of the revelations earlier this year that another US software giant, Lotus, had built an NSA "help information" trapdoor into its Notes system, and that security functions on other software systems had been deliberately crippled.

### 2.6 Windows Firewall with Advanced Security

According (Garmes, 2004), beginning with Windows Vista and Windows Server 2008, configurations of both Windows Firewall and Internet Protocol security (IPsec) are combined into a single tool, the Windows Firewall with Advanced Security MMC snap-in. On by default, Windows Firewall with Advanced Security consolidates and enhances two functions that were managed separately in previous versions of Windows:

Filtering of all IP version 4 (IPv4) and IP version 6 (IPv6) traffic entering or leaving the system. By default, all incoming traffic is blocked unless it is a response to a previous outgoing request from the computer (solicited traffic) or unless it is specifically allowed by a rule created to allow that traffic. By default, all outgoing traffic is allowed, except for service hardening rules that prevent standard services from communicating in unexpected ways. You can choose to allow traffic based on port numbers, IPv4 or IPv6 addresses, the path and name of an application, the name of a service that is running on the computer, or other criteria.

Protecting network traffic entering or exiting the computer by using the IPsec protocol to verify the integrity of the network traffic, to authenticate the identity of the sending and receiving computers or users, and to optionally encrypt traffic to provide confidentiality. In previous versions of Windows, implementations of server or domain isolation sometimes required the creation of a large number of IPsec rules to make sure that required network traffic was protected while still permitting required network traffic that could not be secured with IPsec. This complexity is eased in Windows Server 2008 by a new default behavior that results in a more secure and easier-to-troubleshoot environment.

### 2.7 Neural network techniques

Appling neural networks techniques for comparison and identification. Neural network techniques explain two ways for Comparison: Linear Associative Memory (LAM) and Backprobagation Network (BPN). Now, the backpropagation is successful in iris recognition which is identified by its suggested topology image compression using Artificial Neural Networks is a topic where project is being carried out in various directions towards achieving a generalized and economical network.

Feedforward Networks using Back propagation Algorithm adopting the method of steepest descent for error minimization is popular and widely adopted and is directly applied to image compression. Various research works (Windo, 2005) are directed towards achieving quick convergence of the network without loss of quality of the restored image. In general the images used for compression are of different types like dark image, high intensity image etc. When these images are compressed using Back-propagation Network, it takes longer time to converge. The reason for this is, the given image may contain a number of distinct gray levels with narrow difference with their neighborhood pixels. If the gray levels of the pixels in an image and their neighbors are mapped in such a way that the difference in the gray levels of the neighbors with the pixel is minimum, then compression ratio as well as the convergence of the network can be improved. To achieve this, a cumulative distribution function is estimated for the image and it is used to map the image pixels. When the mapped image pixels are used, the Back-propagation Neural Network yields high compression ratio as well as it converges quickly.

### 2.7.1 Standard Backpropagation (BP)

The Backpropagation BP learns a predefined set of output example pairs by using a two phase propagate adapts cycle. As seen in Figure 2.5, after an input pattern has been applied as a stimulus to first layer of network units, it is propagated through each upper layer until an output is generated. This output pattern is then compared to the desired output, and an error signal is computed for each output unit. The signals are then transmitted backward from the output layer to each unit in the intermediate layer that contributes directly to the output. However, each unit in the intermediate layer receives only a portion of the total error signal, based roughly on the relative contribution the unit made to the original output. This process repeats, layer by layer, until each unit in the network has received an error signal that describes its relative contribution to the total error. We follow Freeman and Skapura’s book (1992) to describe the procedure of training feedforward neural networks using the backpropagation algorithm.

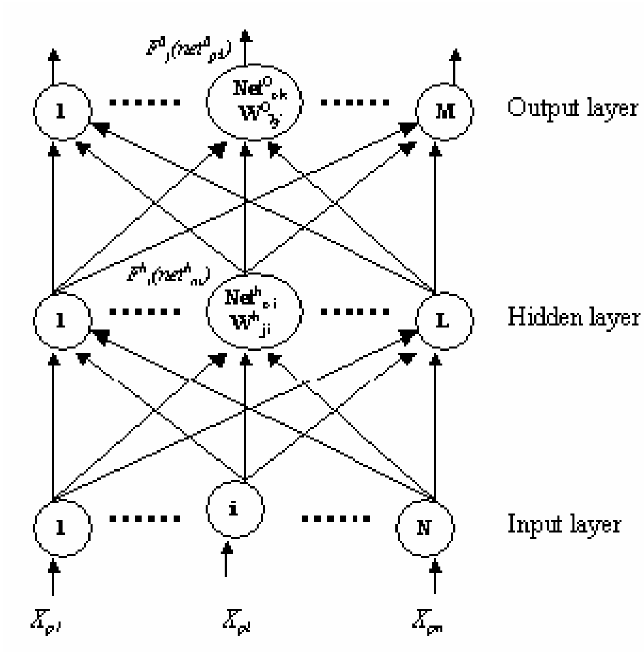



**Figure 2.5:** The Three-layer BP Architecture

The steps of an Object backpropagation:

1. Apply the input example to the input units.

2. Calculate the net-input values to the hidden layer units.

3. Calculate the outputs from the hidden layer.

4. Calculate the net-input values to the output layer units.

5. Calculate the outputs from the output units.

6. Calculate the error term for the output units, but replace new δ°pk with δ°pk (in all equations in appendix).

7. Calculate the error term for the output units, using new δ°pk, also.

8. Update weights on the output layer.

9. Update weights on the hidden layer.

10. Repeat steps from step 1 to step 9 until the error (Ypk – Opk) is acceptably small for each training vector pairs.

# CHAPTER THREE

# METHODOLOGY

Since 1987, when the first relevant methodology was presented by Flom and Safir (Sanderson *et al.,* 2000), many distinct approaches have been proposed. In 1993 Daugman presented one of the most relevant methodologies, constituting the basis for many functioning system. In the segmentation stage, he introduced an integral differential operator to find both the iris inner and outer borders. This operator remains actual and was proposed with some minor difference in 2004 by Nishino and Nayar (Roizenblatt *et al.,* 2004). In a similar from, Camus and Roizenblatt (2004) and (Roche *et al.,* 2005) propose integro differential operators that search over an N3 space having as objective the maximization of equation that identify the iris borders. Wides (2004) proposed iris segmentation through a gradient based binary edge map construction followed by circular Hough transform. This is the most common methodology, being proposed with several minor variants in (Liam *et al.,* 2006) proposed a simple method on the basis of threshold and function maximization in order to obtain tow ring parameters corresponding to the iris inner and outer borders. (Du *et al.,* 2006) have proposed an iris detection method on the basis of prior pupil identification. The image is then transformed into polar coordinates and the iris outer border is identified as the largest horizontal edge resultant from Sobel filtering. This approach may fail in the case of non-concentric iris and pupil, taps well as in very 'dark' iris textures.

Morphologic operators were applied by Mira and Mayer 2005 to obtain iris borders. They detect the inner border by applying threshold and image opening and closing and the outer border by applying threshold, closing and opening sequences. On the basis of the assumption that the image-captured intensity values can be well represented by a mixture of three Gaussian distribution components. (Kim *et al.,* 2004) proposed the use of the expectation maximization algorithm to estimate the respective distribution parameters. They expect that 'dark'. 'intermediate' and 'bright' distributions contain the pixels corresponding to the pupil, iris and reflection areas.

The analysis of the iris recognition literature allowed us to identify tow major strategies for iris segmentation, i.e. using a [1] rigid or deformable template of the iris or [2] its boundary. In most cases, the edge map followed by the application of some geometric from fitting algorithm. The template based strategy usually involves the maximization of some equations and is in general more specific. Based on these facts, we selected four these methodologies the classical boundary based Wides' approach and three of the template approaches (Dagman's, Camus and Wildes' and Martin Roch *et al.,* 2006). These were chosen because of their relevance in the literature, the results presented by the authors and by our belief that they are representative of the majority of the earlier described methodologies. The next sections detail the four selected methodologies, which were implemented and tested on the UBIRIS database.

### 3.1 Daugman's method

This methodology is clearly the most cited in iris recognition literature. It is licensed to Iridian Technologies who turned it into the basis for 99.5% of the present day commercial iris recognition systems. Proposed in 1992, it was the first methodology effectively implemented in a working biometric system. Daugman assumed both pupil and iris with a circular form and applied an integrodifferential operator

$$\max_{r,x_0,y_0} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} \mathrm{d}s \right|$$

This operator searches over the image domain (x, y) for the maximum in the blurred (by a Gaussian kernel Gs(r)) partial derivative with respect to increasing radius r, of the normalized contour integral of I(x, y) along a circular arc ds of radius r and centre coordinates (x0, y0). In practical terms, this method searches in an N3 space for the circumference centre and radius that have the highest derivative value when compared with that of neighbour radius. This process proved to be very effective on images with clear intensity separability between iris, pupil and sclera regions. However, we observed that it frequently fails when images do not have sufficient intensity separability between iris and sclera regions. As possible optimisations, we implemented two pre-process operations that enhanced image contrast and contributed to the improvement of the results.

1. Histogram: equalization: This operation improves the contrast between each eye's regions, thus contributing to the correct algorithm segmentation.
2. Binarisation: applying a threshold on an image before the operator's execution

Enables the maximization of the contrast between the regions belonging to the iris and the remaining ones. This process has, however, one major disadvantage, i.e. it is highly dependent on the threshold chosen and as image characteristics may change, the results may seriously deteriorate. Apart from this fact, the binarisation compromises one of this methodology's biggest advantages: the inexistence of user-defined parameters for the segmentation task.

### 3.2 Wildes' method

This methodology, proposed in 1997 by Wildes, performs its contour fitting in two steps:

1. The image intensity information is converted into a binary edge map.

2. The edge points vote to instantiate particular contour parameter values.

The construction of the edge map is accomplished through the gradient based canny edge detector. In order to incorporate directional tuning, the image intensity derivatives are weighted to favor ranges of orientation. For example, on the iris/sclera border, the derivatives are weighted to be selective for vertical edges. The second step is made through the well-known circular Hough transform where each edge point votes for particular contour parameter values. This methodology is clearly the most common in iris segmentation approaches, having as a principal disadvantage the dependence of threshold values on the edge-map construction. This fact can obviously constitute one weak point as far as the robustness is concerned and includes the ability to deal with heterogeneous image characteristics. Regarding this methodology, we observed that the algorithm and the necessary tuned parameters are critical factors for its accuracy. tested this methodology with three distinct and well-known edge-detector algorithms.

**3.3 Clustering algorithm: For the clustering (**classification iris recognition**)**

Algorithm, the most important feature is its capacity to classify, in the same class, all the pixels belonging to the iris and all the remaining ones in a distinct one. For this purpose, we evaluated four unsupervised clustering and classification algorithms:

Kohonen's self-organizing maps: Also called topological ordered maps, the goal of this algorithm is to represent all points in the source space by points in the target space, such that distance and proximity relationships are preserved as much as possible. The task is this: having an input space and a sequence of input points, to create a mapping from to the target space y such that points neighboring in the source space are mapped to points that are neighboring in y. The map is usually learned by a fully connected neural network where each cell represents a point in the target space. When a pattern from is presented, each cell in the target space computes its net activation and one of the Cells is activated. All weights from this cell and its neighbors are then adjusted in relation to the input pattern as shown in Figure 3.1.

K-means: Having a predefined number of k clusters and n data points, each one with dimension d, the algorithm begins by randomly initializing each coordinate of the k clusters. The distance between data points and clusters is computed and each input corresponds to one activated cluster. The weights of this cluster are adjusted in relation

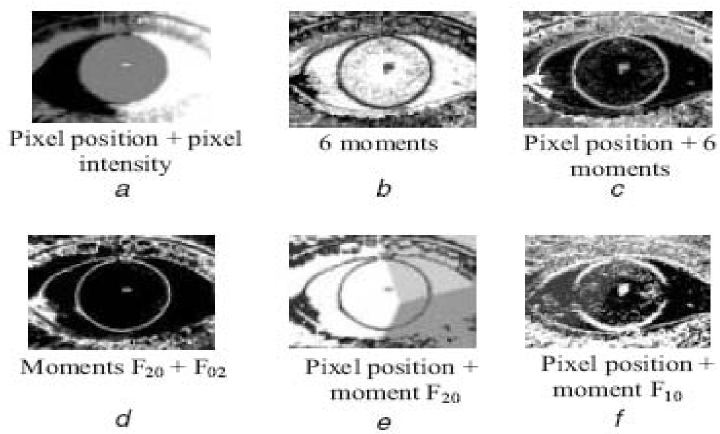



**Figure3.1:** Tested feature sets

To the input so that at the end of each iteration, the distance between data points and clusters is minimal. This process is repeated iteratively until the cluster weights are not adjusted. At this point, the k clusters are returned as the algorithm output. Fuzzy K-means: In every iteration of the classical k-means procedure, each data point is assumed to belong exactly and completely to one cluster. Relaxing this condition, we can think that each sample has a fuzzy membership to each of the k clusters as shown in Table 3.1.

**Table 3.1:** Variants of the proposed algorithm

| **Session 2, %** | **Session 1,%** | **Features** | **Algorithm** |
|---|---|---|---|
| 96.83 | 97.69 | Pixels position intensity | K-means |
| 89.14 | 92.33 | Moments F20 F02 | K-means |
| 96.68 | 97.69 | Pixels position intensity | SOM |
| 90.95 | 95.14 | Moments F20 F02 | SOM |
| 97.88 | 98.02 | Pixels position intensity | Fuzzy K-means |
| 90.04 | 93.90 | Moments F20 F02 | Fuzzy K-means |
| 95.17 | 96.86 | Pixels position intensity | Expectation maximisation |
| 89.14 | 92.17 | Moments F20 F02 | Expectation maximisation |

### 3.4 The mythology for personal recognition (as show Figure 3.2)

The mythology for personal recognition/identification system is composed of the following steps:

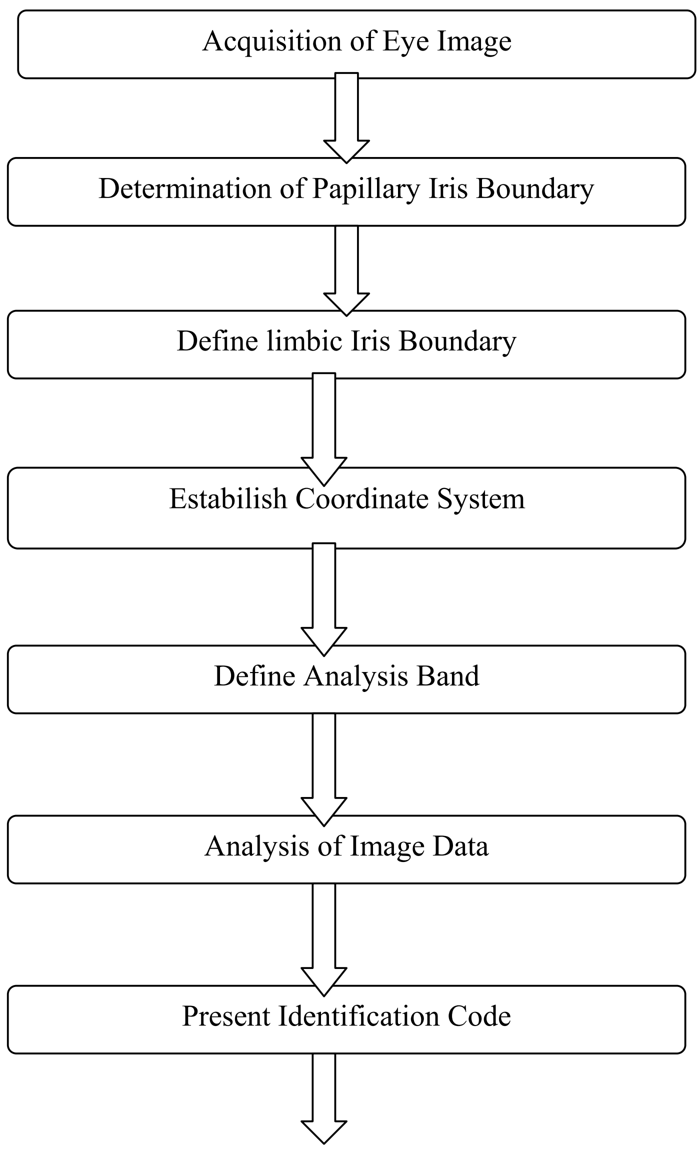
**(Step 1)** *Acquisition of Eye Image:* This is the stage of acquiring the eye image from CCD camera or digital camera.

**(Step 2)** *Determination of Pupillary Iris Boundary:* By utilizing the eye image, the boundary between the pupil and the iris is detected after the position of the eye in the given image is localized.

**(Step 3)** *Definition of Limbic Iris Boundary:* After the center and the radius of the pupil are extracted, the right and the left radius of the iris are searched based on these data.

**(Step 4)** *Establishment of Coordinate System:* By making use of the center and the radius which are calculated in advanced step, we set the polar coordinate system. In this coordinate system, the feature of the iris is extracted.

**(Step 5)** *Recognition/Identification of Iris:* The extracted iris pattern is partitioned into tracks in the form of band. Each local region of these tracks is transformed into complex number with the 2-D Gabor filter. Actually, the sign of real or imaginary part of transformed number is encoded into ‘°1‘± for positive sign and ‘°0‘± for negative sign. The assigned bits are compared with the bits of all personal codes in the data-base or the registered memory. Finally, the system makes a decision to recognize/identify for the given iris by the matching score Iris recognition was developed in the early 1990s by John Daugman at the University of Cambridge. The method analyses individual patterns of the iris and today is mainly used for verification purposes (access control).


Acquisition of Eye Image
Determination of Papillary Iris Boundary
Define limbic Iris Boundary
Estabilish Coordinate System
Define Analysis Band
Analysis of Image Data
Present Identification Code

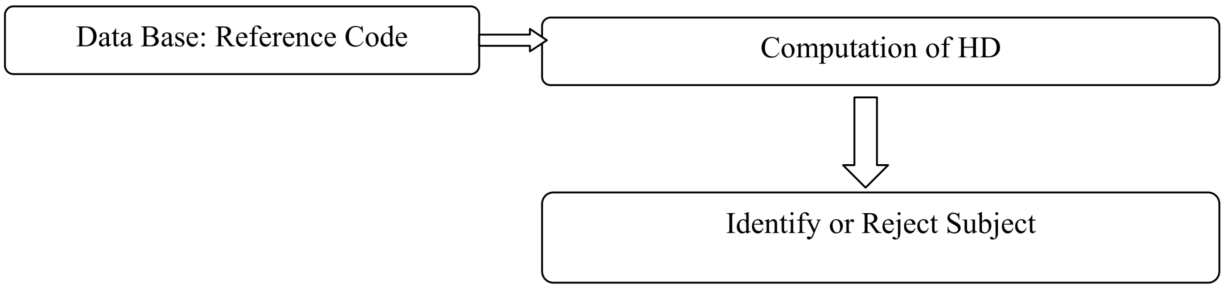



**Figure 3.2:** The overall flow of personal recognition/identification system by using the iris.

A monochrome camera is used to capture the image by near infrared light (NIR) at a distance of 0.1 to 1 meter. The resolution of taken picture varies from 50 to 140 dpi. For the calculation of the so called IrisCode (a string of 2048 bits) e.g. the Daugman Algorithm is used. The following picture shows an example of an iris picture together with a graphical representation of the calculated IrisCode. The comparison of an IrisCode against a stored template is done mainly using the 'Hamming Distance' method as show Figure 3.3.

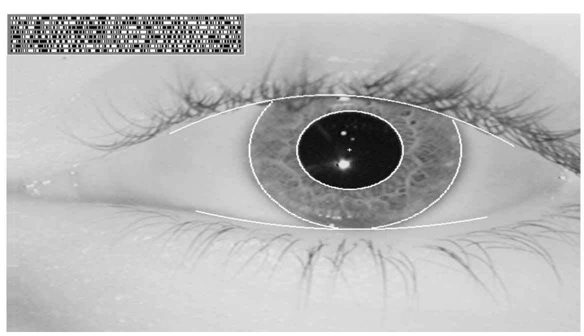


**Figure 3.3:** Picture of an iris and graphical representation of an IrisCode

**3.5 Methodology for Iris recognition system (**as show Figure 3.4**)**

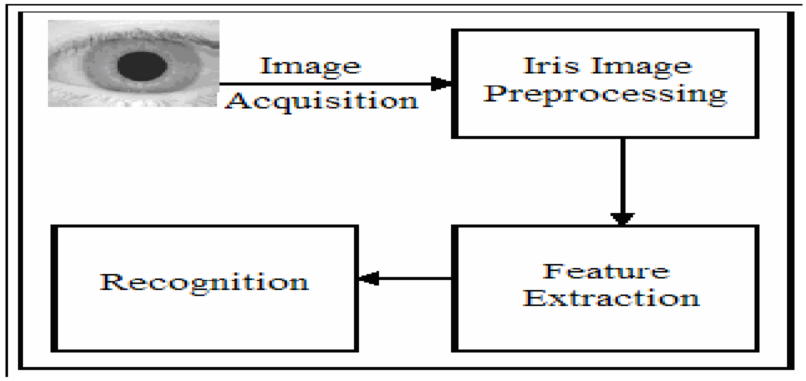



**Figure 3.4:** Iris recognition system methodology

### 3.5.1 Image Acquisition

In iris recognition image acquisition is an important step. Since iris is small in size and dark in color, it is difficult to acquire good image. Also all the subsequent steps depend on it. A Panasonic camera has been used to take eye snaps while trying to maintain appropriate settings such as lighting, distance to the camera and resolution of the image. The image is then changed from RGB to gray level for further processing show as figure 3.5 for Automatically capturing iris images over a range of object distances.

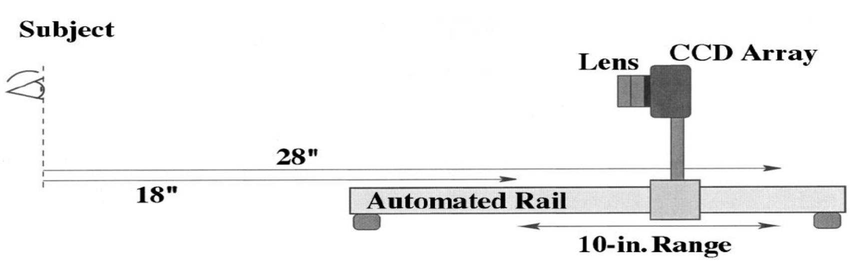



**Figure 3.5:** Automatically capturing iris images

### 3.5.2 Preprocessing

First of all to separate the iris from the image the boundaries of the iris and pupil are detected. Since pupil is the darkest area in the image as shown in Figure 3.6; so a rough estimate of its center (Cx, *C*y) is performed using the following formula

$$C_x = \arg\min_x \left( \sum_y I(x, y) \right)$$
$$C_y = \arg\min_y \left( \sum_x I(x, y) \right)$$

Where *I(x, y)* is the iris image intensity at point (x, y). To find the exact center of the pupil, a part of image is binarized using an adaptive threshold obtained by the histogram of square window size 121*121 pixels with cantered at the estimated center (Cx, *C*y). Then the centriod of the square window is determined which gives the exact center of the pupil. After this, radius of the pupil is obtained by tracing from center of the pupil to the boundary between iris and pupil on different.

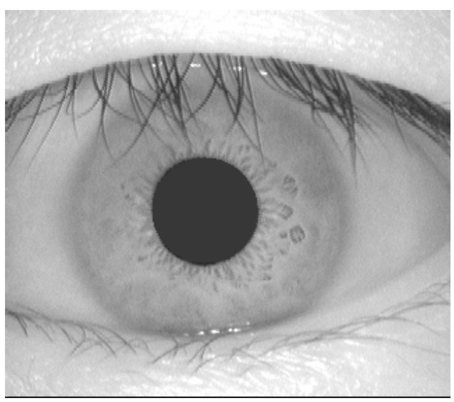


**Figure 3.6:** Image of an iris direction in the binary image and then averaging them.

To detect the boundary between iris and sclera, the image is convolved with a blurring function which is a 2D Gaussian operator with center at (x0, *y*0)

$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x-x_0)^2+(y-y_0)^2}{2\sigma^2}}$$

Where is standard deviation that smoothes the image and then apply canny operator with the threshold values 0.005 and 0.1 as lower and upper limits. Now image is binarized

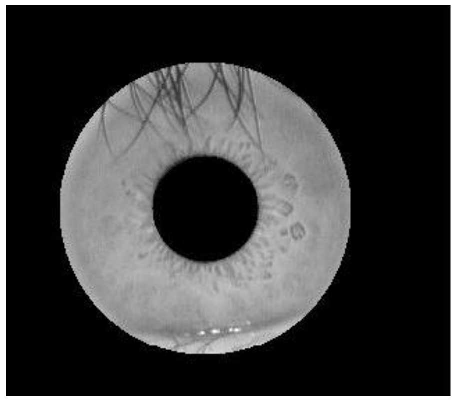


**Figure 3.7:** Localized iris of Figure 3.5 to find the radius of iris with similar way just as for pupil.

These two radii localize the iris as shown in Figure 3.8 then this hollow disk is mapped to a rectangle using following formula.

$$\dot{I}(\dot{x}(r,\theta), y(r,\bar{\theta})) \rightarrow \bar{I}(r,\theta)$$

Where $r$ lies on the unit interval [0, 1] and $r$ is circular angle in [0, 2]. This unwrapping is started from inner to outer boundary of iris, m concentric circles are obtained, then n samples are collected on each concentric circle, so m $r$ n matrix represents the specific flat iris. Every sample started from vertical downward line in the counter clockwise direction, as shown in Figure 3.8 Enhancement of unwrapped iris. The unwrapped flat iris has low contrast. This iris is enhanced by eliminating background and applying histogram equalization. Figure 3.9 shows the result of enhancement of flat iris image.

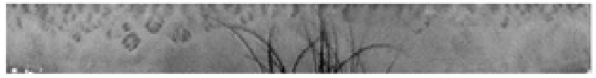


**Figure 3.8:** Unwrapped normalized iris

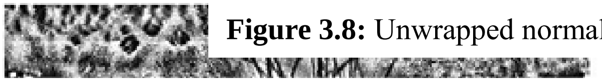


**Figure 3.9:** Enhanced unwrapped iris

### 3.5.3 Feature Extraction

The developed system has been trained to four irises of each class. In the training process mean of trained irises is subtracted from each iris.

$$M_{i \times j} = \frac{1}{k} \sum_{p=1}^{k} I_p$$

Where k is the total number of irises and *Ii* is the it iris image. Eigen vectors are calculated for the outer product of the each iris. Thus, Eigen vector corresponding to the highest Eigen value is used as distinctive feature of the iris.

## 3.6 Design Prototype

### 3.6.1 Software Specification

Microsoft Windows XP SP2, VISTA.

MATLAB V 7.0.

Microsoft Access 2003.

Kenarl

### 3.6.2 Hardware Specification

The prototype was developed using a desktop computer with the following specifications:

Step 1:

Intel Pentium 4 1.8GHz

512 MB RAM

SVGA display adapter

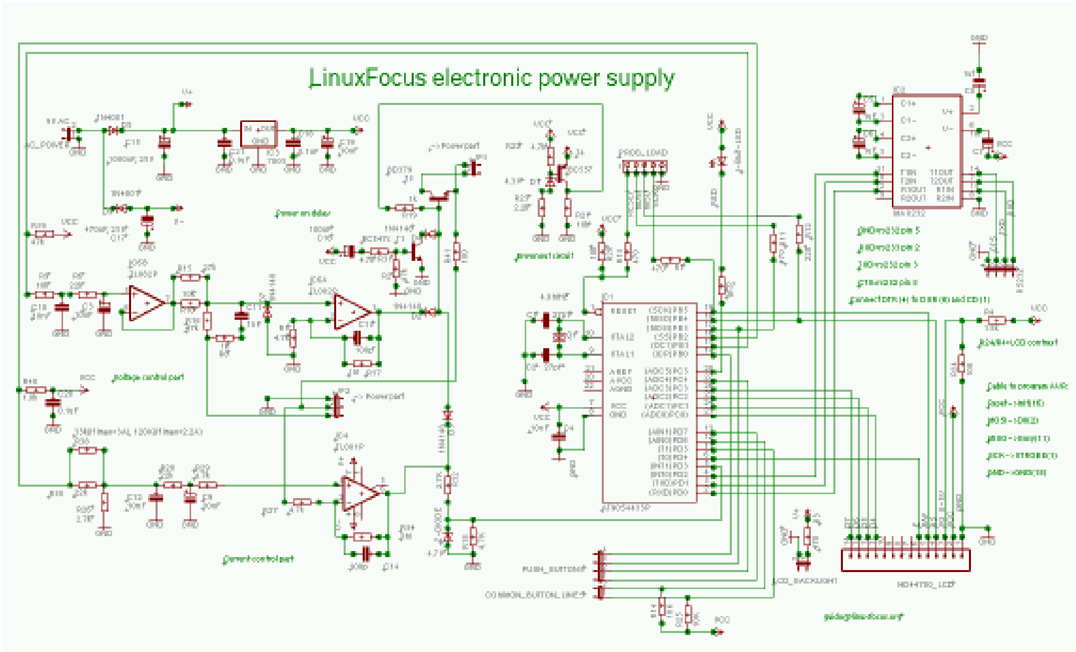
Camera high accuracy

Step 2: as show table 3.2

**Table 3.2:** Hardware Specification

| | |
|---|---|
| Motherboard |  |
| Image Processor with JPEG Encoder CPU |   |
| Diode |   |
| historischer Mikroprozessor vom Typ 80286-10Mhz, produziert von Siemens |  |

Step 3: Map




**3.7 Iris recognition (**as show Figure 3.10**)**

Iris recognition is the only biometric authentication technology specifically designed to work in a one-to many search mode. Authentication speed in dependent on hardware, and there is no degradation of authentication integrity even as database sizes scale into the millions. Unlike other biometric technologies that produce a short list of possible. However the technology performs superbly in verification modes with tokens or PINs.

1. Iris recognition is ideal for use in the one to many search environment because the template is small and the ability to search large databases at speed with accuracy is unmatched by any biometric
2. A live present at the imager results in a conversion of that image to a template that is compared against all other templates in the database.
3. Unlike other biometric technologies, which pull out a set of “possible”, iris

recognition uses the algorithmic parameters to establish only one best match.

4. The probability of misidentification with one eye is 1 in 1.2 million.

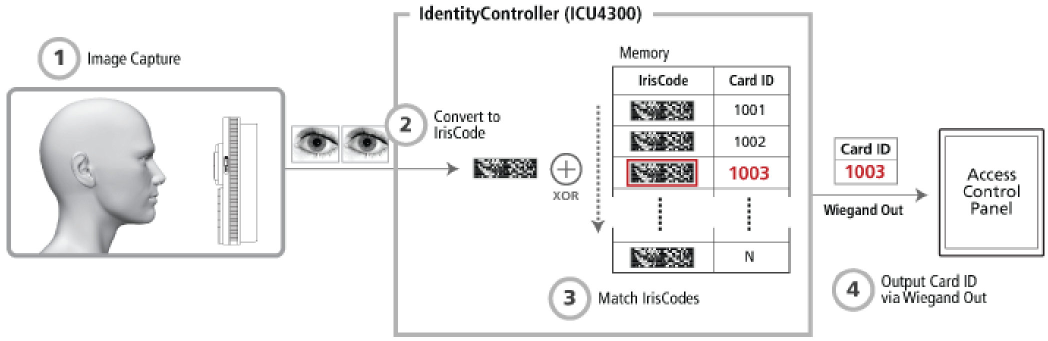



**Figure 3.10:** Identity Controller

### 3.8 Phase based IRIS recognition algorithms

This section describes possible modification of the phase based iris recognition algorithm figure 1shows the baseline algorithm for iris recognition, which consists of a preprocessing stage and a matching stage.

### 3.9 Preprocessing

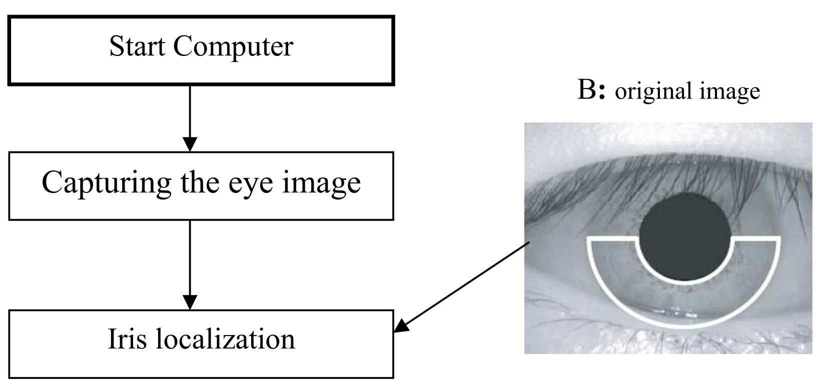
An iris image contains some irrelevant parts (e.g., eyelid, sclera, pupil, etc.). Also, the size of an iris may vary depending on camera-to-eye distance and lighting condition. Therefore, the original image needs to be normalized.

(i) Iris Localization: This step is to detect the inner (iris/pupil) boundary and the outer (iris/sclera) boundary in the original image. We model the inner boundary as an ellipse, and the outer boundary as a circle.

(ii) Iris Normalization: Next step is to normalize iris images to compensate for iris deformation. In order to avoid eyelashes, we use only lower half portion of the iris (Figure 3.11 (b)) and unwrap the region to a rectangular block of a fixed size (128×256 pixels) as illustrated in Figure 3.11 (c). The eyelid region is then masked (d) as show Figure 3.12 and 3.13.

### 3.10 Matching

The key idea of the algorithm is to use phase-based image matching for image alignment and matching score calculation (see Figure 3.11).



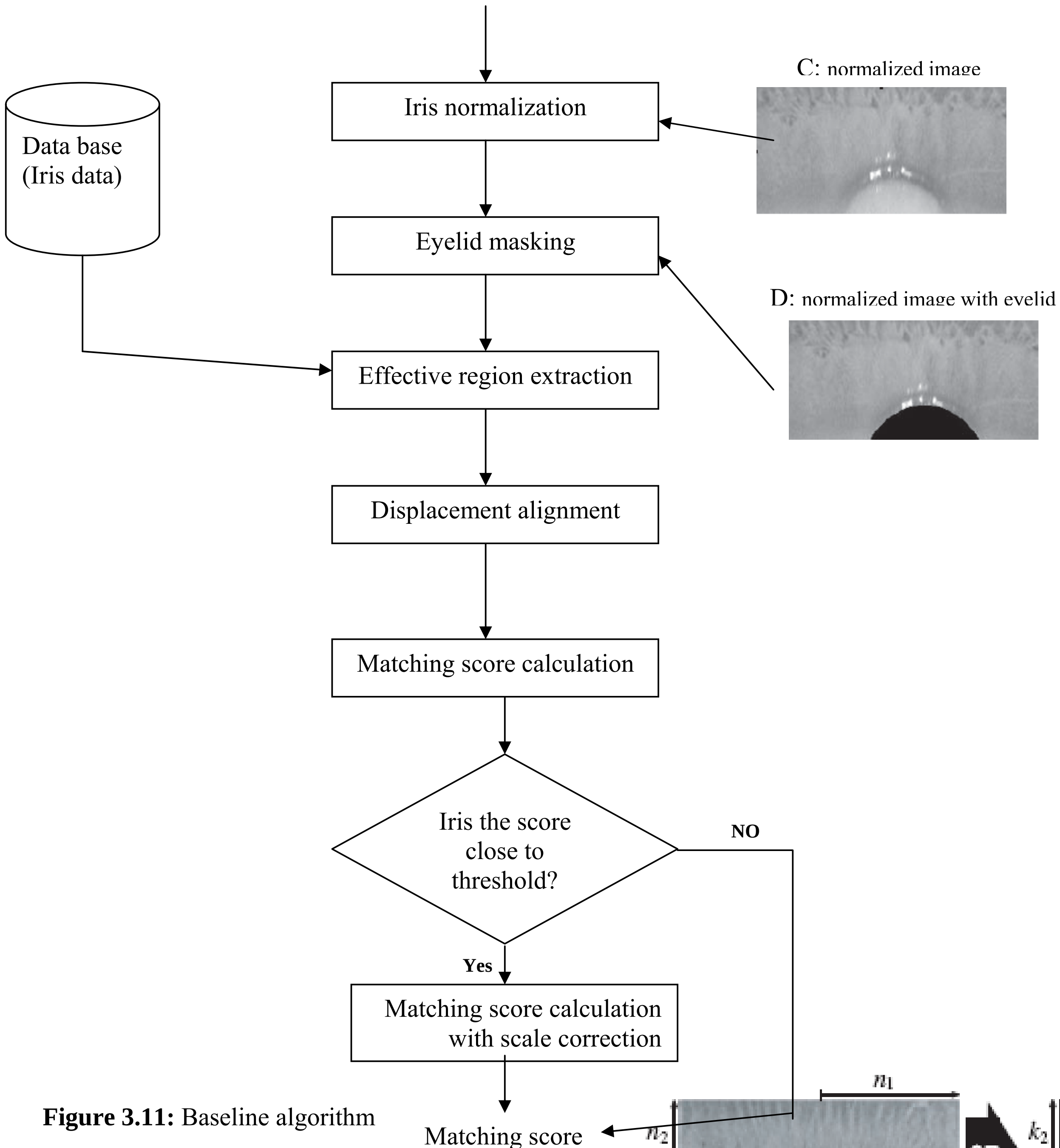



**Figure 3.11:** Baseline algorithm

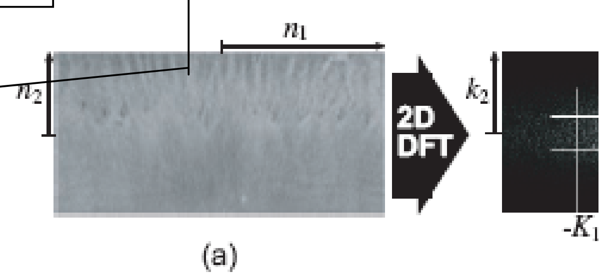



**Figure 3.12**: Normalized iris image in (a) spatial domain, and in (b) frequency domain (amplitude spectrum), where $K1 = 0.55M1$ and

$K2 = 0.2M2$.

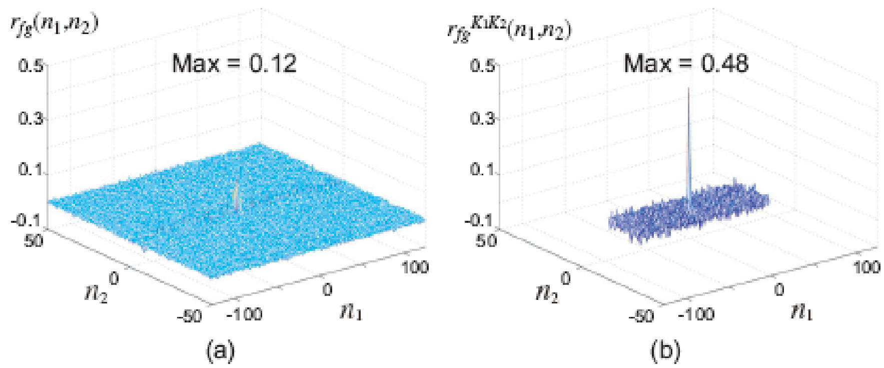



**Figure 3.13:** Example of genuine matching using the original POC function and the BLPOC function: (a) original POC function $r_{fg}(n1, n2)$, and (b) BLPOC function $r^{K1K2}_{fg}(n1, n2)$.

### 3.10.1 Effective region extraction

The purpose of this process is to extract the effective regions of the same size as illustrated in Figure 3.14 (a). When the extracted region becomes too small to perform image matching, we extract multiple effective sub-regions from each iris image by changing the width parameter w (Figure 3.14 (b)). Extract 6 sub-regions from an iris image by changing the parameter w as 55, 75 and 95 pixels.

(i) Displacement alignment: This step is to align the translational displacement between the extracted regions. The displacement parameters can be obtained from the peak location of the BLPOC

(ii) Matching score calculation: calculate the BLPOC function between the aligned images and evaluate the matching score as the maximum correlation peak value. When multiple sub-regions are extracted as illustrated in Figure 3.16 (b), the matching score is calculated by taking an average for effective sub-regions. If the matching score is close to threshold value to separate genuines and impostors, we calculate the matching score with scale correction.

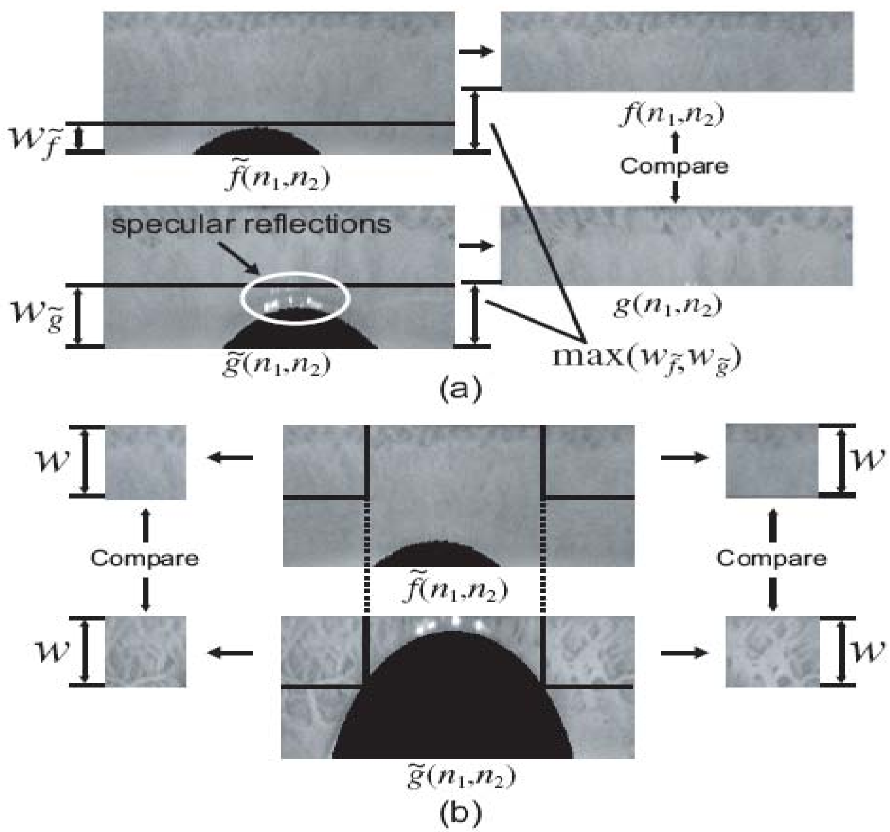



**Figure 3.14:** Effective region extraction: (a) normal case, (b) case when multiple sub regions should be extracted.

### 3.11 Automatic iris recognition system

Implement automatic iris recognition system, algorithm in both iris detection and feature extraction modes. Using morphological operators for pupil detection and selecting the appropriate radius around the pupil to pick the region of iris which contains the collarets that appears as a zigzag pattern are the main contributions. This region provides a unique textual pattern for feature extraction. Selected coefficients of 3-level and 3-level Dubieties wavelet decompositions of iris images are chosen to generate a feature vector. To save the storage space and computational time for manipulating the feature vector, we quantize each real value into binary value using merely its sign disregarding its magnitude. A typical iris recognition system includes some major steps as depicted in Figure 3.15. At first, an imaging system will be designed to capture a sequence of iris images from the subject in front of camera. The next step is choosing a clear image from the sequence of captured images. A good iris quality assessment based on Fourier spectra analysis after selecting the high-quality image, with morphological image processing operators, the edge of the pupil is determined. A brief overview of the method is as follows:

1 Filling the holes which are pseudo created by the light reflection on the cornea or further in eye.

2 Enhancing the contrast of image by adjusting image intensity,

3 Finding the “regional minima.” Regional minima are connected components of pixels with the same intensity value, T, whose external boundary pixels all have a value greater than T.

4 Applying morphological operators. The operation is repeated until the image

no longer changes and sets a pixel to 1 if five or more pixels in its 3-by-3 neighborhood are 1's; otherwise, it sets the pixel to 0 in a binary image.

5 A removing the small connected parts in image which their areas are less than a threshold.

The pupil now is well detected and its center and radius are gotten. We can also obtain the edge of iris that is mentioned. The advantage of this kind of edge detection is its speed and good performance because in morphological processing, we deal with binary images and processing on binary images is very fast. After pupil detection, with trial and error, we get that by choosing an appropriate radius as the outer boundary of iris, the selected region by this threshold contains the collarets structure well. Preprocessing on the selected iris region that includes iris normalization, iris image enhancement and denoising.

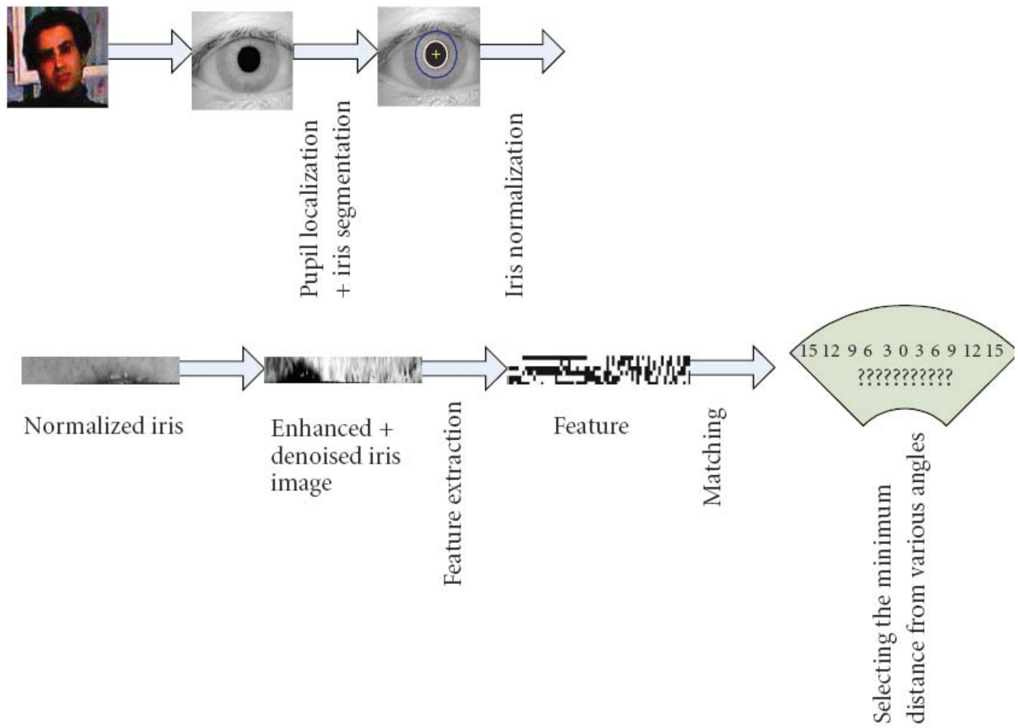
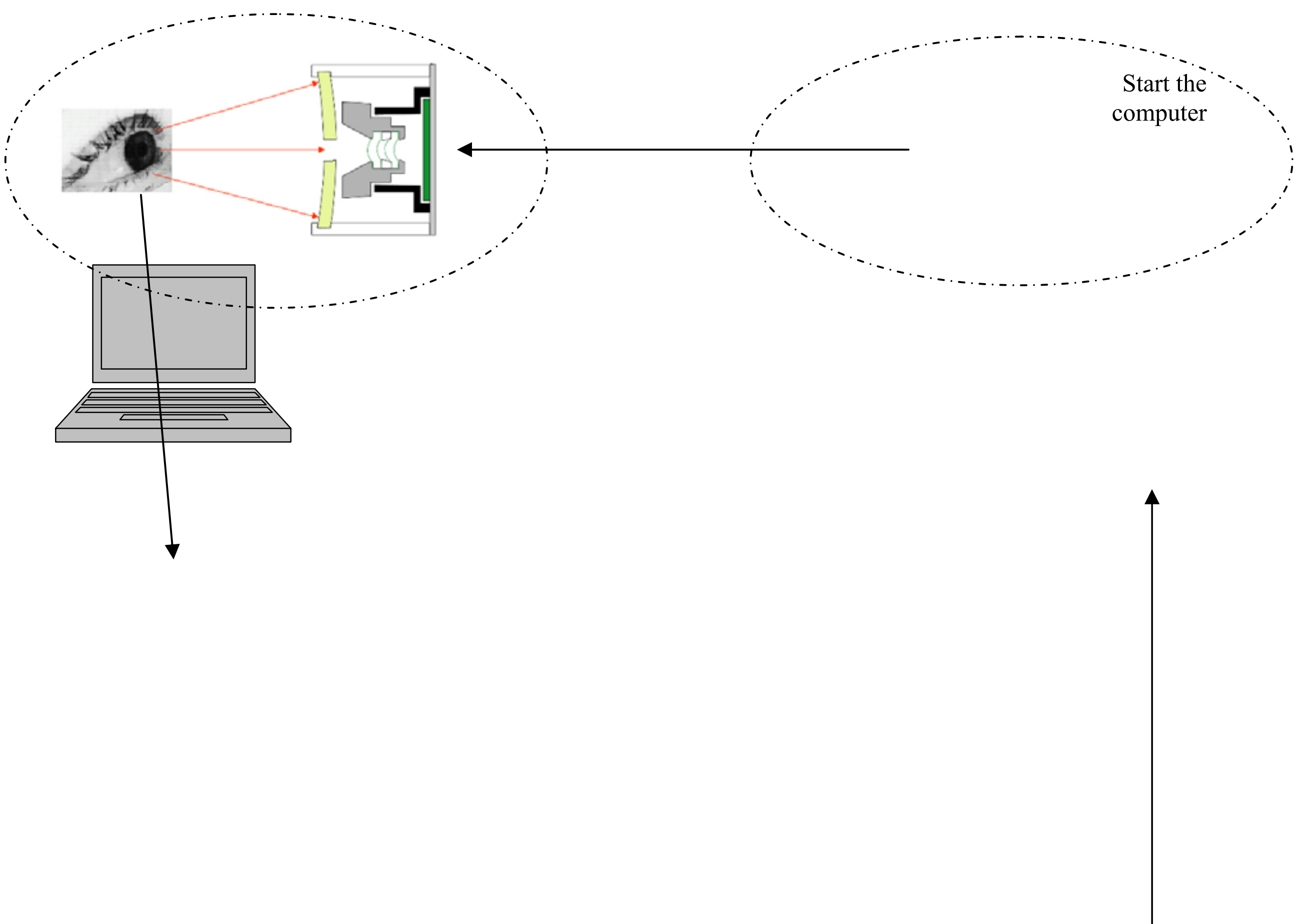



**Figure 3.15:** Flowchart of automatic iris recognition system.

**3.12 Block Diagram (**as show Figure 3.16**)**



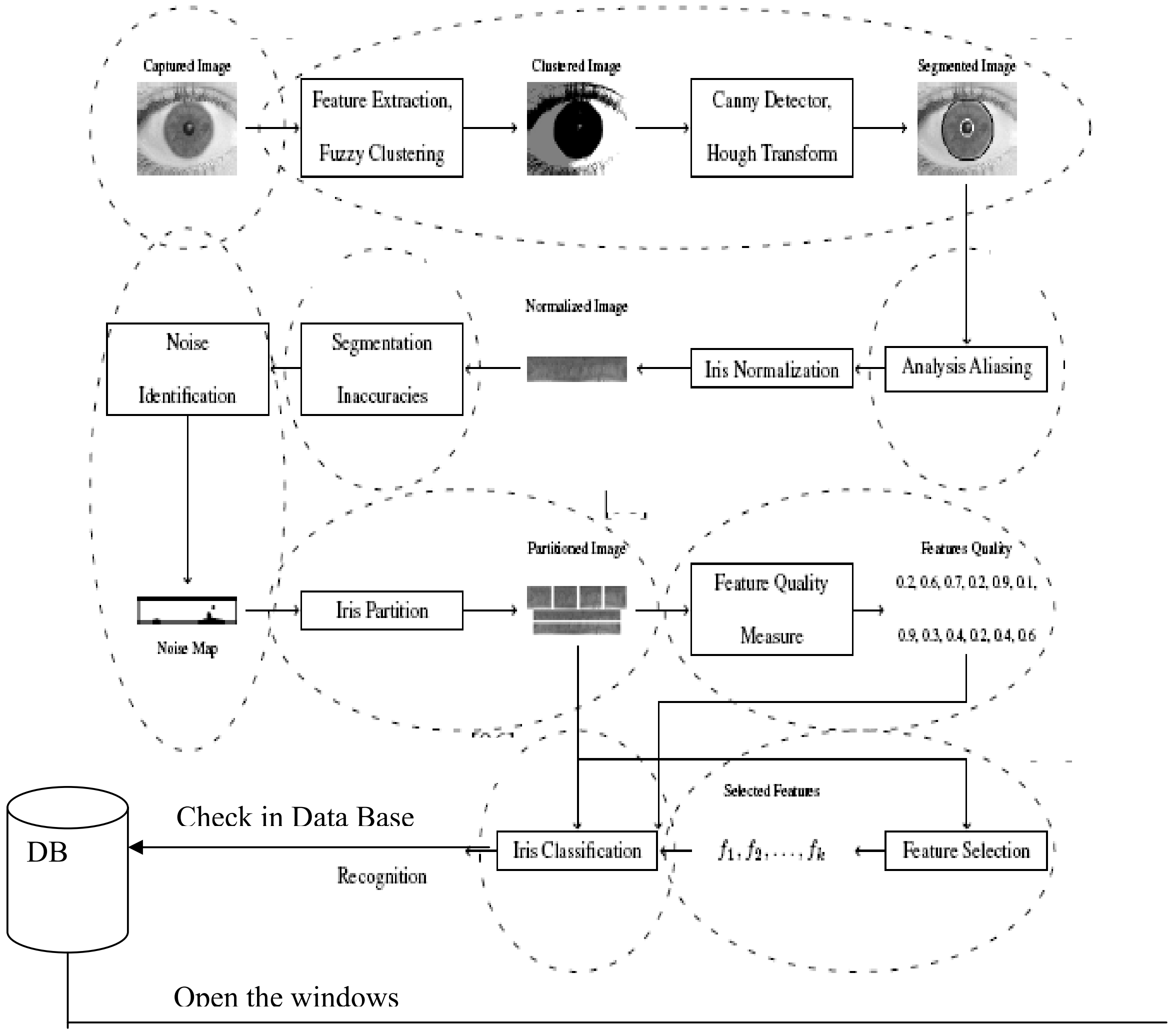



**Figure3.16:** Block Diagram access windows

1. The construction of a new iris image database, for research purposes
2. A more robust iris segmentation method, able to deal with highly heterogeneous and noisy iris images. This method is suitable for its application in the non-cooperative image capturing setting.
3. The influence that small iris segmentation errors have in the final recognition accuracy and the proposal of a method able to identify these inaccuracies.
4. The analysis of the probability of aliasing in the iris normalization stage and the identification of the maximum and minimum sampling rates that must be used in the process to avoid this problem and identification of noise regions in

normalized iris images. This method produces a binary map that can be used in further stages, namely in the feature extraction, comparison and selection.

5. An iris classification based on the iris partition, in the independent feature extraction on each partition and in the further iris classification through a fusion rule. This strategy avoids that localized noise regions in the iris images corrupt the whole biometric signature and degrade the recognition accuracy.
6. A feature quality measure, used in the feature comparison stage.

### 3.13 Types of Noise in the Captured Iris Images

This section is especially relevant in the context of our work. Here we identify and describe the most common noise factors that result of non-cooperative image capturing processes, either at-a-distance, without users' cooperation and within heterogeneous lighting conditions. Based in observations of the available iris image databases and in our experimental imaging processes, we identified eleven factors that we considered as noise: the iris obstruction by eyelids (NEO) or eyelashes (NLO), specular (NSR) or lighting reflections (NLR), poor focused images (NPF), partial (NPI) or out-of iris images (NOI), off-angle iris (NOA), motion blurred irises (NMB) and pupil (NPS) or sclera (NSS) portions wrongly considered as belonging to the iris.

#### 3.13.1 Iris obstructions by eyelids (NEO)

The biological function and natural eyelid movement can obstruct relevant portions of the iris, especially in its vertical extremes. Commonly, NEO noise regions are one of the largest and appear in the lower regions of the segmented and normalized iris images.

$$C = \sum nX \; ||g_{\_,r}|| - {}_{n}X_{\_=\_+1} \; (||g_{\_,r} - g_{\_,r}||) - I_{\_,r} \; n$$

### 3.13.2 Iris obstructions by eyelashes (NLO)

Eyelashes can obstruct portions of the iris in two distinct forms as they appear isolated or grouped. If an eyelash is isolated (upper eyelid of Figure 3.18), it appears as a very thin and darker line in the iris region. The existence of multiple eyelashes in the iris regions generates a uniform darker region (near the upper eyelid of Figure 3.17).

$$D = \sum_{m} \left( \sum_{k=1}^{5} (I_{n,m} - I_{n-k,m}) \right)$$

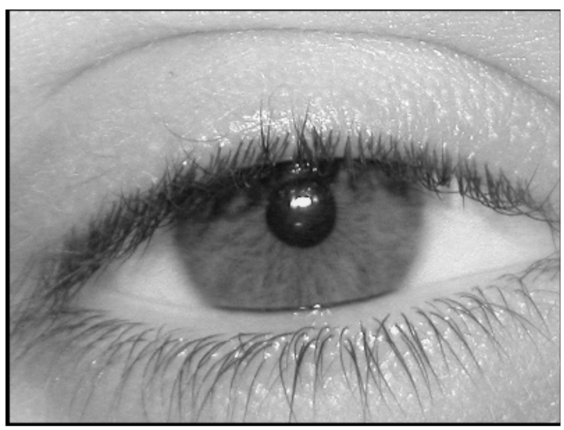


**Figure 3.17:** Noisy iris image due to eyelids and eyelashes obstructions.

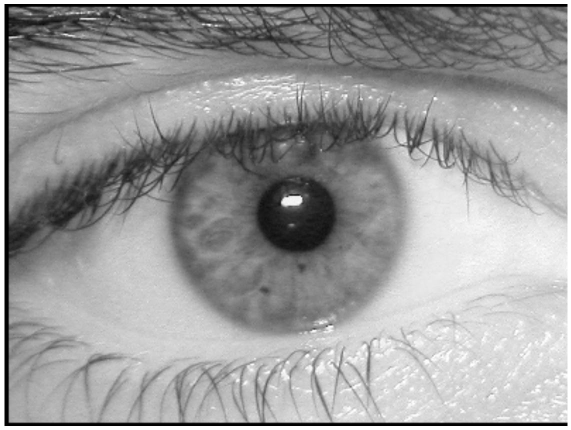


**Figure 3.18**: Noisy iris image due to isolated eyelashes obstructions.

### 3.13.3 Lighting reflections (NLR)

These types of noise regions usually correspond to reflections from artificial light sources near to the subject, although they can appear in the image capturing within natural lighting environments. These reflections have high heterogeneity, as they can appear with a broad range of dimensions and localized in distinct regions of the iris. These areas have intensity values close to the maximum and are exemplified by the region on the upper and left portion of the iris of Figure 3.19.

$$M_{pq} = \sum_{-W/2}^{W/2} ( \sum_{-W/2}^{W/2} (I(m,n) x_m^p y_n^q))$$

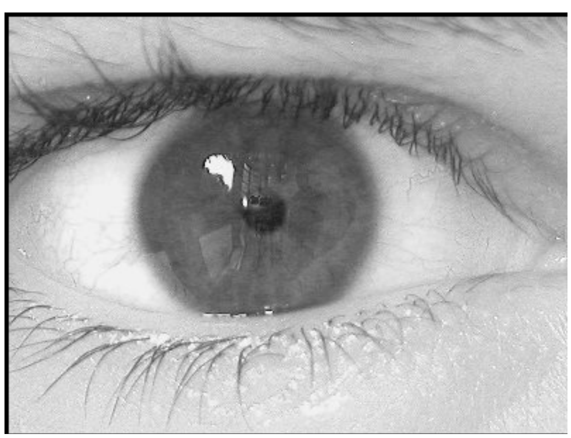


**Figure 3.19:** Noisy iris image due lighting reflections.

### 3.13.3 Specular reflections (NSR)

These types of reflections correspond to reflected information from the environment where the user is located or is looking at. As illustrated by the highest intensity region in the upper portion of the iris of Figure 3.20, these reflections can obstruct large regions, or even the majority, of the iris. Commonly, they have lower intensity values than the lighting reflections and can correspond to a wide range of objects that the user is surrounded by.

$$F_{pq}(i,j) = \frac{1}{L^2} \sum_{(a,b)\in W_{ij}} (tanh(\sigma(M_{pq}(a,b) - \bar{M}))$$

### 3.13.5 Poor focused images (NPF)

Due to the moving elements that interact in the non-cooperative capturing and to the limited depth-of-field of any imaging system, the image focus is

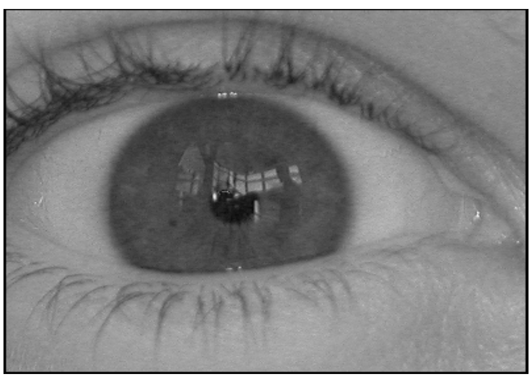


**Figure 3.20:** Noisy iris image due specular reflections.

One of the biggest concerns. Sometimes, small deviations (centimeters) in the image Capturing distance can propitiate the existence of images with severe focus problems that, almost invariably, lead to the increment of the false rejection rates. A poor focused image is illustrated by Figure 3.21.

$$J_{fuz} = \sum_{i=1}^{c} \left( \sum_{j=1}^{n} (\hat{P}(w_i|x_j, \hat{\theta})^b ||x_j - \mu_i||^2) \right)$$

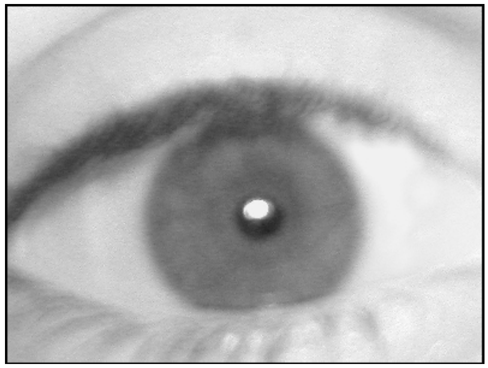


**Figure 3.21:** Noisy iris image due to poor focus

### 3.13.6 Partial captured irises (NPI)

The image capturing at a distance and with subjects head And body movements propitiates that the close-up eye images could contain exclusively portions of the iris. Depending of the amount of information missing, this can be obviously a relevant obstacle to biometric recognition, which is illustrated by Figure 3.22.

$$f(x|\theta) = \sum_{j=1}^{L} (w_j f_j(x|\theta_j))$$

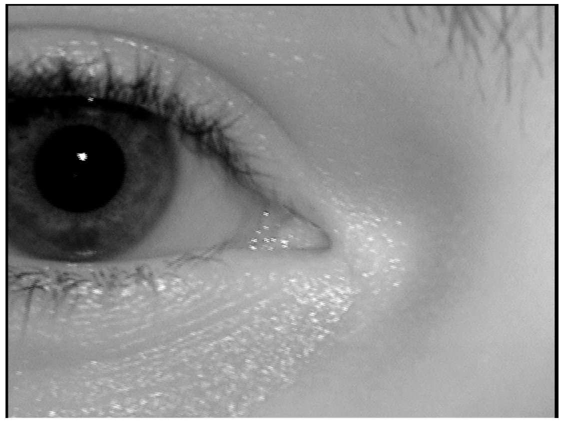


**Figure 3.23:** Partial captured iris.

### 3.13.7 Out-of-iris images (NOI)

This is an extreme noisy factor and, obviously, obstructs any attempt of biometric recognition. However, it must be considered, in order to avoid false acceptances motivated by the execution of the recognition algorithms based in non-iris areas. An example of a capture without any portion of the iris visible is shown in Figure 3.25.

$$P(x) = \prod_{i=1}^{N} \Big( \sum_{j=1}^{L} (w_j f_j(x|\theta_j)) \Big)$$

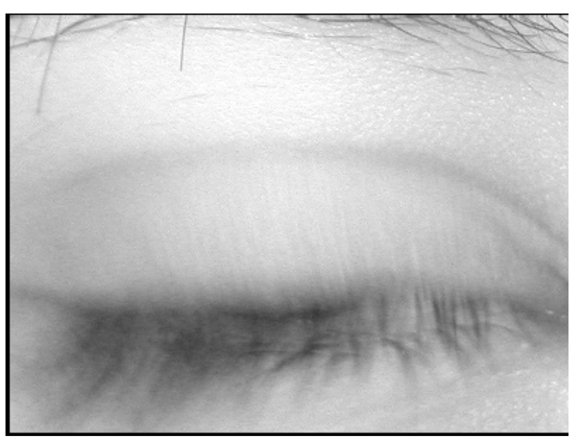


**Figure 3.23:** Out-of-iris image.

### 3.13.8 Off-angle iris (NOA)

Due to rotation of the subjects head and eyes, it is possible to capture iris images with the iris not aligned with the imaging direction, as exemplified by Figure 3.24. These off-angle images have elliptical shape for the region corresponding to the iris. They demand the use of projection techniques, in order to deal with the iris data as if it was not off-angle.

$$I \oplus S := \bigcup \{x : S + x \in I\}$$

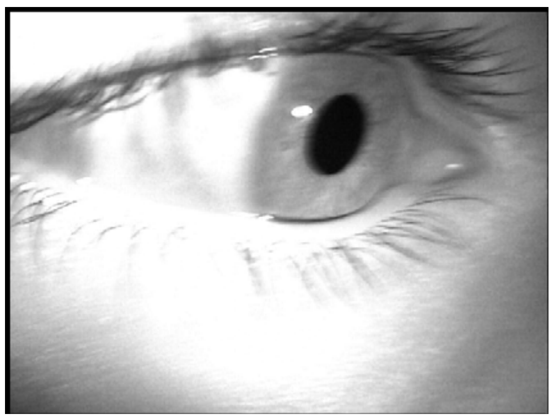


**Figure 3.24:** Off-angle iris image.

### 3.13.9 Motion blurred images (NMB)

Once again due to several moving parts that interact in the iris image capturing; the iris image can be blurred by motion. Since it is the most frequent and quickest type of interacting movement, we observed that the eyelids movement has a significant contribute to this type of noise, as illustrated by Figure 3.25.

$$a_k = \frac{1}{w*w}\sum_{i=0}^{w-1}\Big(\sum_{j=k*w}^{(k+1)*w-1} I(i,j)\Big).$$

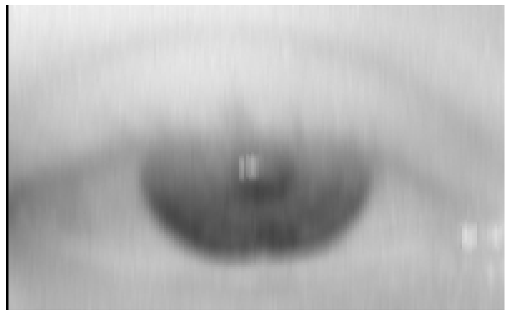


**Figure 3.25:** Motion blurred iris image

### 3.13.10 Pupil wrongly considered as belonging to the iris (NPS)

When the segmentation of the pupillary iris border is not accurate, some portions of the iris will be wrongly considered as belonging to the iris. Those areas appear at the upper part of the normalized and segmented iris image and have usually lower intensity values than those that correspond to the iris, as exemplified by Figure 3.26.

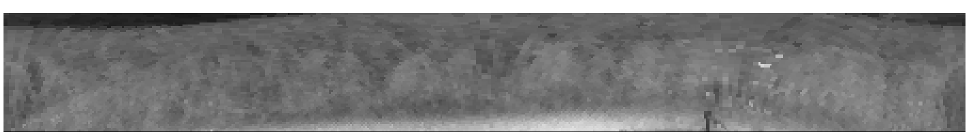


**Figure 3.26:** Normalized iris image with a translation error on the pupil segmentation

### 3.13.11 Sclera wrongly considered as belonging to the iris (NSS)

Similarly to the above described type of noise, when the segmentation of the scleric iris border is not accurate, portions of the sclera are wrongly considered as belonging to the iris and appear in the lower part of the segmented and normalized iris images.

The analysis of the above described noise factors allowed us to divide them into two major classes: local and global. The first correspond to noise that corrupts localized regions of the image, whereas the remaining regions remain noise-free and possibly enable the execution of the recognition task. As described in the following chapters, the detection, localization and robust handling of local noise factors can significantly improve the robustness of iris recognition and represent an achievement towards non-cooperative recognition. Oppositely, the global noise factors affect the image as a whole and, depending of its intensity, can constitute a definitive obstacle to the recognition process.

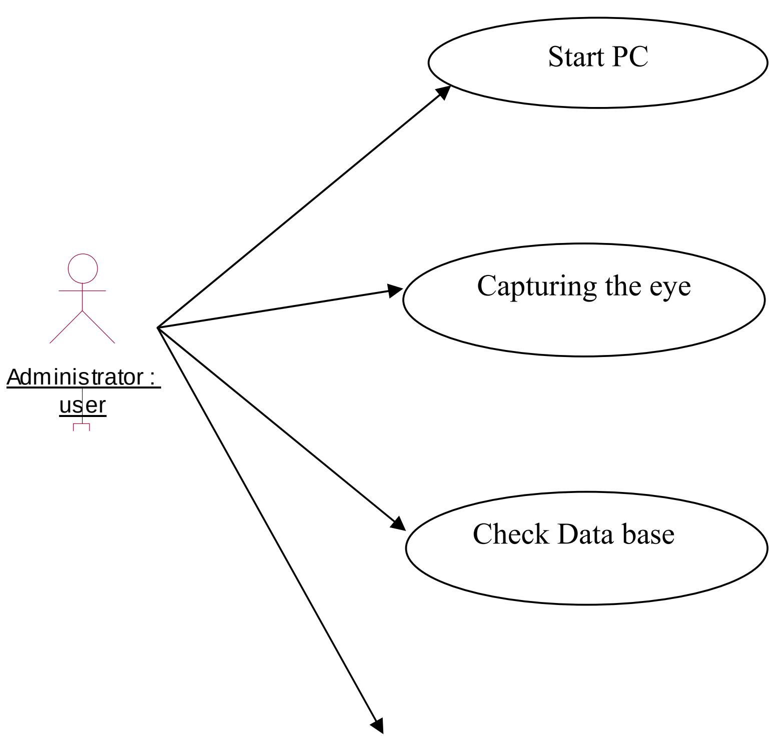
# CHAPTER FOUR

# RESULTS

This chapter presents the results of integrating neural network in iris recognition system. The chapter begins by explaining about the Use Case Diagram as well as Sequence Diagram. The detail experimental results of neural networks training and testing are also presented and discussed.

## 4.1 Use Case Diagrams

According to Wikipedia.org, A use case is a technique for documenting the potential requirements of a new system or software change. Each use case provides one or more scenarios that convey how the system should interact with the end user or another system to achieve a specific business goal. Use cases are deceptively simple tools for describing the behavior of software or systems. A use case contains a textual description of all of the ways which the intended users could work with the software or system. Use cases do not describe any internal workings of the system, nor do they explain how that system will be implemented. They simply show the steps that a user follows to perform a task. All the ways that users interact with a system can be described in this manner. Many people cannot differentiate a Use Case from a Use Case Diagram. Use case diagrams are often confused with use cases; while the two concepts are related, use cases are far more detailed than use case diagrams. In one word, a use case diagram is used to demonstrate the functions that the web information system could provide and the extent to which a student can interact using those functions. In the other hand, a use case is the description of functions of the iris information system from the user and Administrator point of view. UML use-cases and UML class diagrams have been produced from the analysis and design stages respectively; these are best described as follows; Use Cases A scenario is a sequence of steps describing an interaction between computer and user. A use-case then is a set of scenarios tied together by a common user goal as show Figure 4.1.



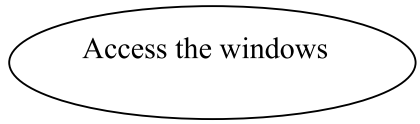



**Figure 4.1:** Use Case Diagrams for access windows by iris recognition

## 4.2 Sequence diagram

A Sequence diagram depicts the sequence of actions that occur in a system. The invocation of methods in each object, and the order in which the invocation occurs is captured in a Sequence diagram. This makes the Sequence diagram a very useful tool to easily represent the dynamic behavior of a system as show Figure 4.2.

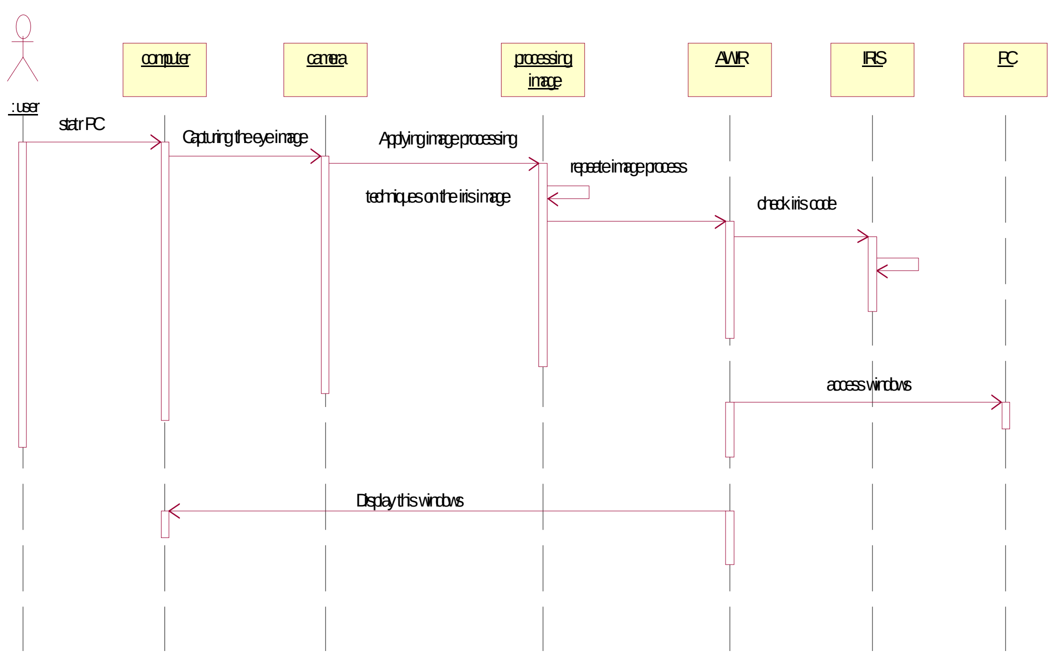


**Figure 4.2:** Sequence diagram for access widows by iris recognition

### 4.3 Neural Networks Experiments

A number of experiments were performed to show the effectiveness of the developed algorithm, using Pentium IV 2.8 GHz processor. A total of 20 different eyes (i.e. different iris classes) were tested and for each iris seven images were used. This makes up a total of 140 experiments. The system was so trained to four images and remaining three images of each class were used as test images. The correct recognition Rate of this system is 94.28%. Experiments while varying the number

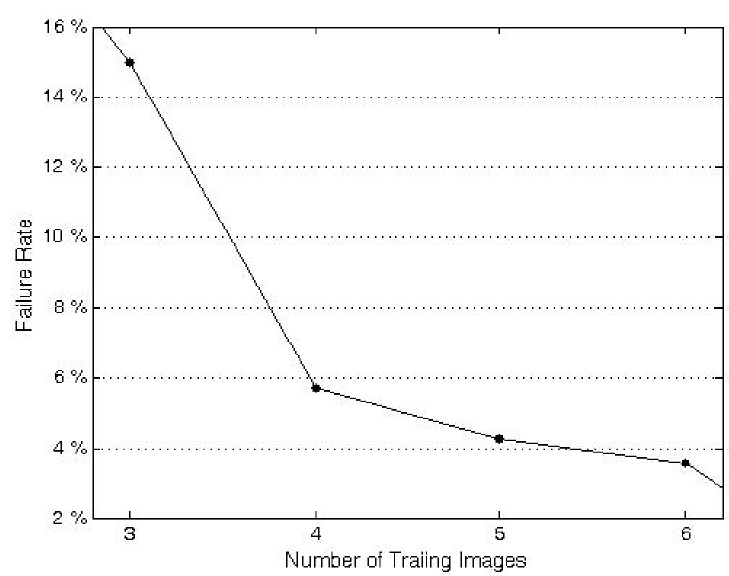



**Figure 4.3:** Number of training images vs. failure rate

Of training images were also carried out. Some results are depicted graphically in Figure 4.3. The graphical representation reflects that as the number of training images is increased the rate of failure is decreasing as system is better trained. Similarly the speed of CPU for training is increased as we train the iris more and more.

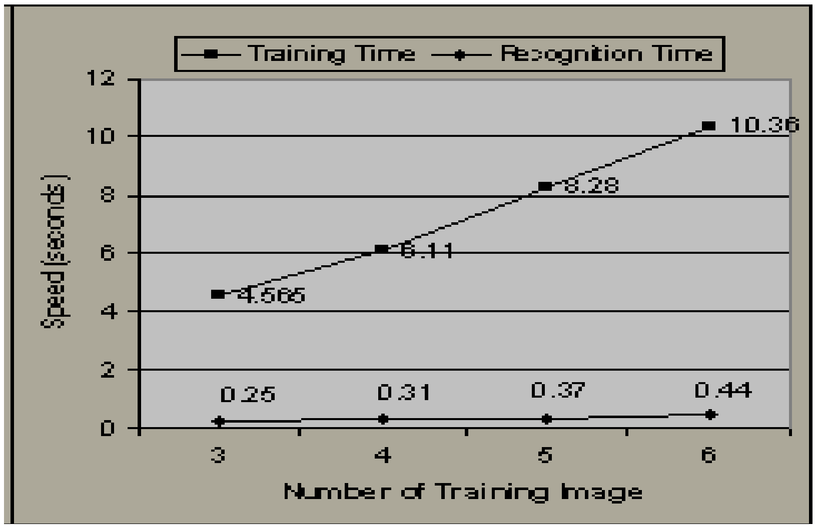
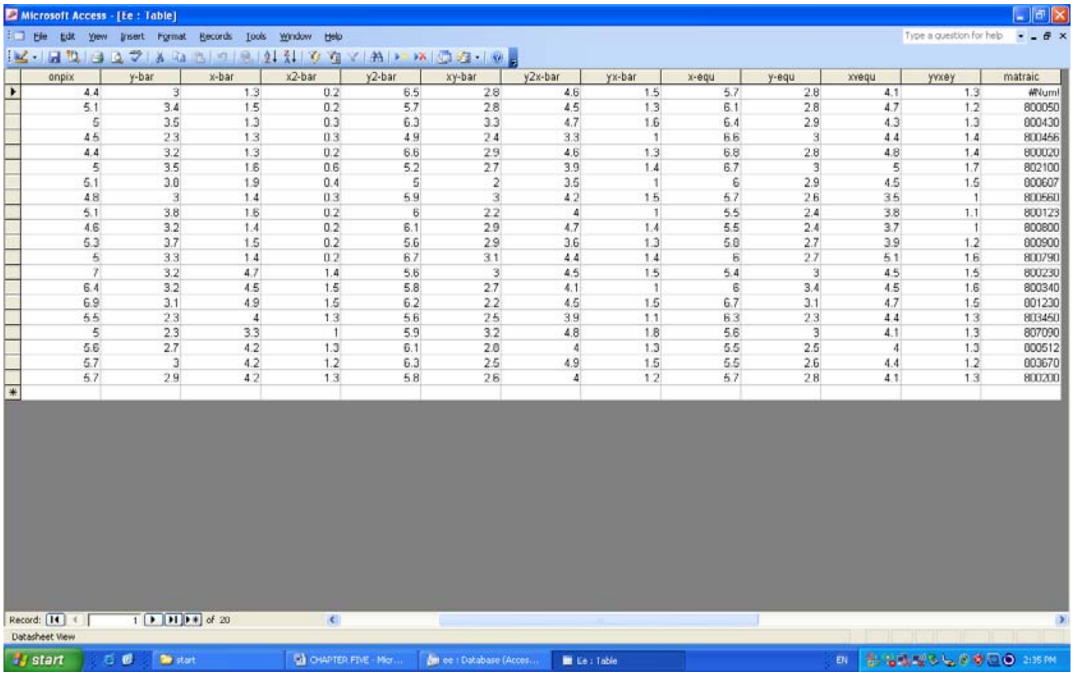



**Figure 4.4:** Number. Of training images

Speed and recognition also varies with respect to number of training Images because CPU requires more time for training as Number of images increases as shown in Figure 4.4. and Figure 4.5. Training Database.



| onpix | y-bar | x-bar | x2-bar | y2-bar | xy-bar | y2x-bar | yx-bar | x-equ | y-equ | xvequ | yvxey | matraic |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.4 | 3 | 1.3 | 0.2 | 6.5 | 2.8 | 4.6 | 1.5 | 5.7 | 2.8 | 4.1 | 1.3 | #Num! |
| 5.1 | 3.4 | 1.5 | 0.2 | 5.7 | 2.8 | 4.5 | 1.3 | 6.1 | 2.8 | 4.7 | 1.2 | 800050 |
| 5 | 3.5 | 1.3 | 0.3 | 6.3 | 3.3 | 4.7 | 1.6 | 6.4 | 2.9 | 4.3 | 1.3 | 000430 |
| 4.5 | 2.3 | 1.3 | 0.3 | 4.9 | 2.4 | 3.3 | 1 | 6.6 | 3 | 4.4 | 1.4 | 800456 |
| 4.4 | 3.2 | 1.3 | 0.2 | 6.6 | 2.9 | 4.6 | 1.3 | 6.8 | 2.8 | 4.8 | 1.4 | 800020 |
| 5 | 3.5 | 1.6 | 0.6 | 5.2 | 2.7 | 3.9 | 1.4 | 6.7 | 3 | 5 | 1.7 | 802100 |
| 5.1 | 3.8 | 1.9 | 0.4 | 5 | 2 | 3.5 | 1 | 6 | 2.9 | 4.5 | 1.5 | 000607 |
| 4.8 | 3 | 1.4 | 0.3 | 5.9 | 3 | 4.2 | 1.5 | 6.7 | 2.6 | 3.5 | 1 | 800560 |
| 5.1 | 3.8 | 1.6 | 0.2 | 6 | 2.2 | 4 | 1 | 5.5 | 2.4 | 3.8 | 1.1 | 800123 |
| 4.6 | 3.2 | 1.4 | 0.2 | 6.1 | 2.9 | 4.7 | 1.4 | 5.5 | 2.4 | 3.7 | 1 | 800800 |
| 5.3 | 3.7 | 1.5 | 0.2 | 5.6 | 2.9 | 3.6 | 1.3 | 5.8 | 2.7 | 3.9 | 1.2 | 000900 |
| 5 | 3.3 | 1.4 | 0.2 | 6.7 | 3.1 | 4.4 | 1.4 | 6 | 2.7 | 5.1 | 1.6 | 800790 |
| 7 | 3.2 | 4.7 | 1.4 | 5.6 | 3 | 4.5 | 1.5 | 5.4 | 3 | 4.5 | 1.5 | 800230 |
| 6.4 | 3.2 | 4.5 | 1.5 | 5.8 | 2.7 | 4.1 | 1 | 6 | 3.4 | 4.5 | 1.6 | 800340 |
| 6.9 | 3.1 | 4.9 | 1.5 | 6.2 | 2.2 | 4.5 | 1.5 | 6.7 | 3.1 | 4.7 | 1.5 | 801230 |
| 6.5 | 2.3 | 4 | 1.3 | 5.6 | 2.5 | 3.9 | 1.1 | 6.3 | 2.3 | 4.4 | 1.3 | 803450 |
| 5 | 2.3 | 3.3 | 1 | 5.9 | 3.2 | 4.8 | 1.8 | 5.6 | 3 | 4.1 | 1.3 | 807090 |
| 5.6 | 2.7 | 4.2 | 1.3 | 6.1 | 2.8 | 4 | 1.3 | 5.5 | 2.5 | 4 | 1.3 | 000512 |
| 5.7 | 3 | 4.2 | 1.2 | 6.3 | 2.5 | 4.9 | 1.5 | 5.5 | 2.6 | 4.4 | 1.2 | 803670 |
| 5.7 | 2.9 | 4.2 | 1.3 | 5.8 | 2.6 | 4 | 1.2 | 5.7 | 2.8 | 4.1 | 1.3 | 800200 |

**Figure 4.5:** Training Database.

## 4.4 Iris Recognition Data Using Neural Network (Data Preprocessing)

It is changed from Iris to letter as shown down using NN to get this result and applying 8 just from 20 images because not enough this paper.

### 4.4.1 Dataset (Example)

| Lettr | x-box | y-box | width | high | onpix | x-bar | y-bar | x2bar | y2bar | xybar | x2ybr | xy2br | x-ege |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | 2 | 8 | 3 | 5 | 1 | 8 | 13 | 0 | 6 | 6 | 10 | 8 | 0 |
| I | 5 | 12 | 3 | 7 | 2 | 10 | 5 | 5 | 4 | 13 | 3 | 9 | 2 |
| D | 4 | 11 | 6 | 8 | 6 | 10 | 6 | 2 | 6 | 10 | 3 | 7 | 3 |
| N | 7 | 11 | 6 | 6 | 3 | 5 | 9 | 4 | 6 | 4 | 4 | 10 | 6 |
| G | 2 | 1 | 3 | 1 | 1 | 8 | 6 | 6 | 6 | 6 | 5 | 9 | 1 |
| S | 4 | 11 | 5 | 8 | 3 | 8 | 8 | 6 | 9 | 5 | 6 | 6 | 0 |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | 4 | 2 | 5 | 4 | 4 | 8 | 7 | 6 | 6 | 7 | 6 | 6 | 2 |

### 4.4.2 Description of Data

4.4.2.1 Target and Attributes

i. Description of attributes

| Attributes | Data Type | Range | | |
|---|---|---|---|---|
| | | Min | Max | Set |
| Iris | Character | | | A To T |
| x-box | Integer | 0 | 15 | |
| y-box | Integer | 0 | 15 | |
| width | Integer | 0 | 15 | |
| high | Integer | 0 | 15 | |
| onpix | Integer | 0 | 15 | |
| x-bar | Integer | 0 | 15 | |
| y-bar | Integer | 0 | 15 | |
| x2bar | Integer | 0 | 15 | |
| y2bar | Integer | 0 | 15 | |
| xybar | Integer | 0 | 15 | |
| x2ybar | Integer | 0 | 15 | |
| xy2bar | Integer | 0 | 15 | |
| x-ege | Integer | 0 | 15 | |

ii. Description of target:

i. What is the target? Our Target is the Iris

ii. How many target values? 20

iii. Class Distribution

**i. A: 39**

**ii. B: 38**

**iii. C: 37**

**iv. D: 40**

**v. E: 38**

**vi. F: 39**

**vii. G: 39**

**viii. H: 37**

**ix. I: 38**

**x. J: 37**

**xi. K: 37**

**xii. L: 38**

**xiii. M: 40**

**xiv. N: 39**

**xv. O: 38**

**xvi. P: 40**

**xvii. Q: 38**

**xviii. R: 38**

**xix. S: 37**

**xx. T: 40**

### 4.4.3 Data Preprocessing

4.4.3.1 Data Selection

i. Original Data

| lettr | x-box | y-box | width | High | Onpix | x-bar | y-bar | x2bar | y2bar | xybar | x2ybr | xy2br | x-ege |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | 2 | 8 | 3 | 5 | 1 | 8 | 13 | 0 | 6 | 6 | 10 | 8 | 0 |
| I | 5 | 12 | 3 | 7 | 2 | 10 | 5 | 5 | 4 | 13 | 3 | 9 | 2 |
| D | 4 | 11 | 6 | 8 | 6 | 10 | 6 | 2 | 6 | 10 | 3 | 7 | 3 |
| N | 7 | 11 | 6 | 6 | 3 | 5 | 9 | 4 | 6 | 4 | 4 | 10 | 6 |
| G | 2 | 1 | 3 | 1 | 1 | 8 | 6 | 6 | 6 | 6 | 5 | 9 | 1 |
| S | 4 | 11 | 5 | 8 | 3 | 8 | 8 | 6 | 9 | 5 | 6 | 6 | 0 |
| B | 4 | 2 | 5 | 4 | 4 | 8 | 7 | 6 | 6 | 7 | 6 | 6 | 2 |

ii. Selected Data

| lettr | x-box | y-box | Width | high | Onpix | x-bar | y-bar | X2bar | y2bar | xybar | x2ybar | xy2bar | x-ege |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N | 3 | 6 | 3 | 4 | 3 | 8 | 7 | 4 | 1 | 6 | 6 | 8 | 5 |
| J | 3 | 9 | 4 | 7 | 4 | 9 | 6 | 3 | 6 | 11 | 4 | 7 | 0 |
| L | 4 | 8 | 5 | 6 | 3 | 5 | 6 | 1 | 9 | 6 | 4 | 6 | 1 |
| J | 3 | 6 | 4 | 4 | 2 | 6 | 6 | 1 | 4 | 12 | 8 | 10 | 1 |
| J | 5 | 9 | 6 | 7 | 4 | 7 | 6 | 2 | 4 | 12 | 8 | 10 | 1 |
| L | 3 | 6 | 4 | 4 | 2 | 5 | 6 | 1 | 9 | 6 | 4 | 7 | 0 |

As mentioned before we had 20 records of data. But, now we combined some records because some values of some attributes are not 20% of the maximum value in the same attribute. In addition, this merging operation made the interval of most of the attributes to change from (0 to 15) to some other different intervals. This issue will be shown in the next part.

### 4.4.4 Data Representation

- Letter( Iris):

A = 1

B = 2

C = 3

D = 4

E = 5

F = 6

G = 7

H = 8

I = 9

J = 10

K = 11

L = 12

M = 13

N = 14

O = 15

P = 16

Q = 17

R = 18

S = 19

T = 20

- x-box:

  1,2,3,4,5,6,7

- y-box:

  1,2,3,4,5,6,7,8,9,10,11

- width:

  2,3,4,5,6,7,8

- high:

1, 2,3,4,5,6,7,8

- onpix:

  1,2,3,4,5,6,7

- x-bar:

  5,6,7,8,9

- y-bar:

  6, 7,8,9,10,11

- x2bar:

  1, 2,3,4,5,6,7,8

- y2bar:

  1,2,3,4,5,6,7,8,9

- xybar:

  6,7,8,9,10,11,12

- x2ybar:

  4,5,6,7,8,9

- xy2bar;

  6,7,8,9,10

- x-ege:

  0,1,2,3,4,5,6

Changed the data representation of the target attribute only. It is changed from letters (Iris) to numbers as shown down. Other attributes remain as they are since they will be processed in the normalization section.

### 4.4.5 Data Normalization

i. normalized values

| Lettr | x-box | y-box | Width | high | onpix | x-bar | y-bar | x2bar | y2bar | xybar | x2ybar | xy2bar | x-ege |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 0.43 | 0.55 | 0.38 | 0.50 | 0.43 | 0.89 | 0.64 | 0.50 | 0.11 | 0.50 | 0.67 | 0.80 | 0.83 |
| 10 | 0.43 | 0.82 | 0.50 | 0.88 | 0.57 | 1.00 | 0.55 | 0.38 | 0.67 | 0.92 | 0.44 | 0.70 | 0.00 |
| 12 | 0.57 | 0.73 | 0.63 | 0.75 | 0.43 | 0.56 | 0.55 | 0.13 | 1.00 | 0.50 | 0.44 | 0.60 | 0.17 |
| 10 | 0.43 | 0.55 | 0.50 | 0.50 | 0.29 | 0.67 | 0.55 | 0.13 | 0.44 | 1.00 | 0.89 | 1.00 | 0.17 |
| 10 | 0.71 | 0.82 | 0.75 | 0.88 | 0.57 | 0.78 | 0.55 | 0.25 | 0.44 | 1.00 | 0.89 | 1.00 | 0.17 |
| 12 | 0.43 | 0.55 | 0.50 | 0.50 | 0.29 | 0.56 | 0.55 | 0.13 | 1.00 | 0.50 | 0.44 | 0.70 | 0.00 |
| 6 | 0.57 | 0.73 | 0.50 | 0.75 | 0.43 | 0.56 | 1.00 | 1.00 | 0.44 | 1.00 | 1.00 | 0.60 | 0.00 |

Converted all the data includes the target attribute to be in the range (0 -1) and converted them by dividing each single number by the maximum in the same attribute. For maximum attribute in the target attribute is 20. So, divided every number in the target attribute by 18.

### 4.4.6 Results

i. Raw Data

| Lettr | x-box | y-box | Width | High | onpix | x-bar | y-bar | x2bar | y2bar | xybar | x2ybr | xy2br | x-ege |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | 2 | 8 | 3 | 5 | 1 | 8 | 13 | 0 | 6 | 6 | 10 | 8 | 0 |
| I | 5 | 12 | 3 | 7 | 2 | 10 | 5 | 5 | 4 | 13 | 3 | 9 | 2 |
| D | 4 | 11 | 6 | 8 | 6 | 10 | 6 | 2 | 6 | 10 | 3 | 7 | 3 |
| N | 7 | 11 | 6 | 6 | 3 | 5 | 9 | 4 | 6 | 4 | 4 | 10 | 6 |
| G | 2 | 1 | 3 | 1 | 1 | 8 | 6 | 6 | 6 | 6 | 5 | 9 | 1 |
| S | 4 | 11 | 5 | 8 | 3 | 8 | 8 | 6 | 9 | 5 | 6 | 6 | 0 |
| B | 4 | 2 | 5 | 4 | 4 | 8 | 7 | 6 | 6 | 7 | 6 | 6 | 2 |

ii. Preprocessed Data

| Lettr | x-box | y-box | width | high | onpix | x-bar | y- | x2bar | y2bar | xybar | x2ybar | xy2bar | x- |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | bar | | | | | | ege |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0.54 | 0.43 | 0.55 | 0.38 | 0.50 | 0.43 | 0.89 | 0.64 | 0.50 | 0.11 | 0.50 | 0.67 | 0.80 | 0.83 |
| 0.38 | 0.43 | 0.82 | 0.50 | 0.88 | 0.57 | 1.00 | 0.55 | 0.38 | 0.67 | 0.92 | 0.44 | 0.70 | 0.00 |
| 0.46 | 0.57 | 0.73 | 0.63 | 0.75 | 0.43 | 0.56 | 0.55 | 0.13 | 1.00 | 0.50 | 0.44 | 0.60 | 0.17 |
| 0.38 | 0.43 | 0.55 | 0.50 | 0.50 | 0.29 | 0.67 | 0.55 | 0.13 | 0.44 | 1.00 | 0.89 | 1.00 | 0.17 |
| 0.38 | 0.71 | 0.82 | 0.75 | 0.88 | 0.57 | 0.78 | 0.55 | 0.25 | 0.44 | 1.00 | 0.89 | 1.00 | 0.17 |
| 0.46 | 0.43 | 0.55 | 0.50 | 0.50 | 0.29 | 0.56 | 0.55 | 0.13 | 1.00 | 0.50 | 0.44 | 0.70 | 0.00 |
| 0.23 | 0.57 | 0.73 | 0.50 | 0.75 | 0.43 | 0.56 | 1.00 | 1.00 | 0.44 | 1.00 | 1.00 | 0.60 | 0.00 |

### 4.5 Access windows by iris recognition

This section explains the timing taken for entering windows 4.2.2 Access windows. Figure 4.6 shows the access windows speed by iris. It verifies that iris recognition is better than other biometrics due to the speed. As explained in figure 4.2, as several iris training is increased, the recognition speed becomes faster which leads to less processing job. So, access windows by iris recognition are very fast and effective.

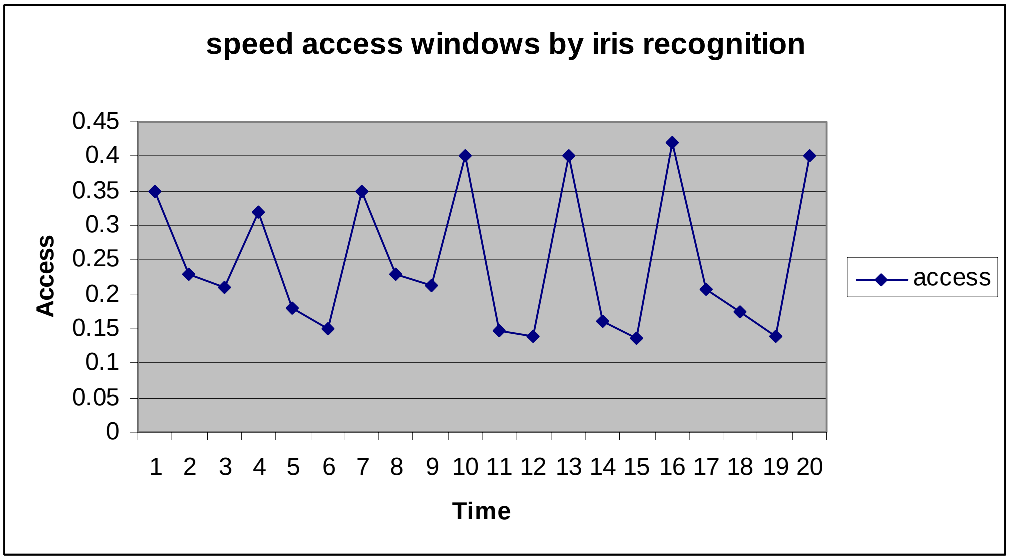



**Figure 4.6:** Comparative between the time and accuracy of image processor

### 4.6 The accuracy of Image

Figure 4.7 shows the image accuracy and capturing versus speed. As capturing process is increased the accuracy is increased as well. This depends on the used camera.

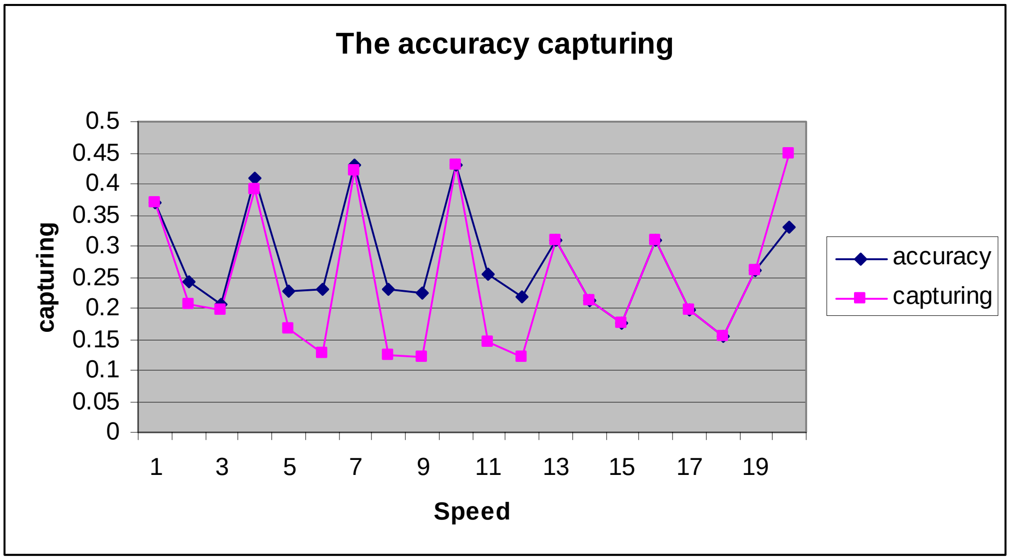



**Figure 4.7:** Comparative between speed and accuracy of the use of image camera with high accuracy

**4.7 Check Iris in Data Base (**as show Figure 4.8)

The used database contains iris codes of persons that are allowed to access a specific laptop. MATLAB 7.0 is used in order to compare a person iris with the database. Figure 4.8 shows the relationship between the database sizes with the speed comparison.

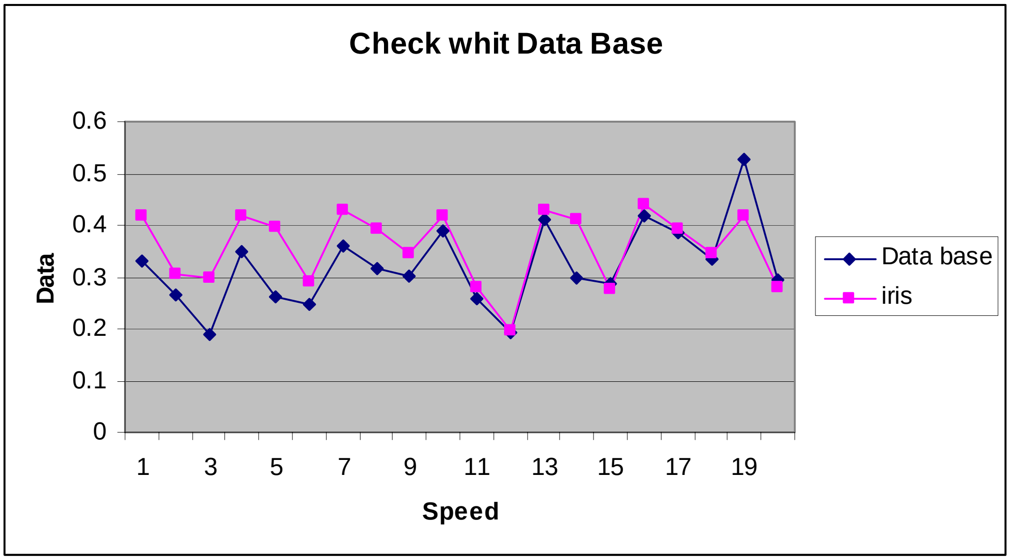



**Figure 4.8:** Comparative research in Data Base entry or the new interface to speed

### 4.8 Processor

Processor the Iris and convert to code as show Figure 4.9. Convert each iris into code to be stored in the database is a very critical step. This conversion is done after taking the iris image directly. It is converted by extracting 160 parameter from each image. In addition, cleaning noise for picture is also done in the same step. Figure 4.6 shows the graph of processing the iris versus the consumed time.

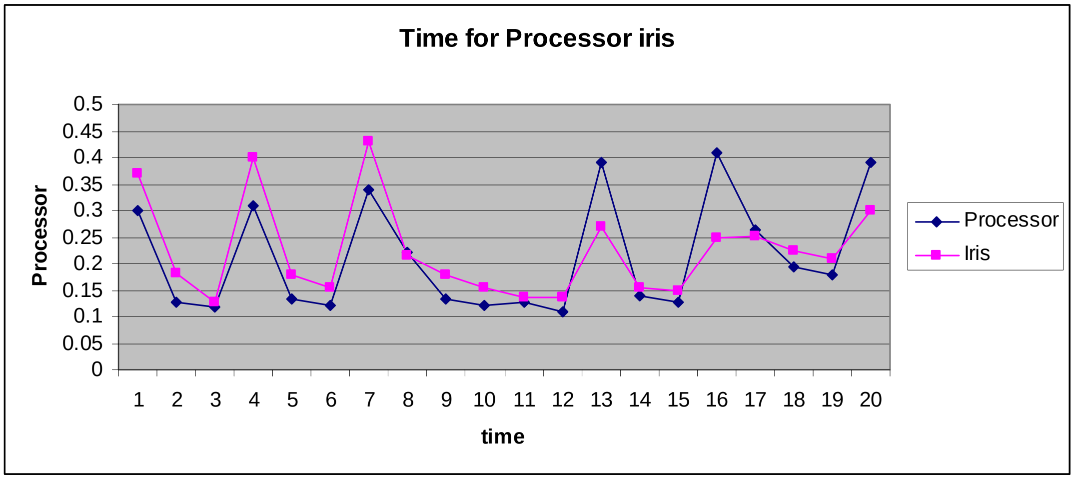



**Figure 4.9:** Comparative between the time and accuracy of image processor

### 4.9 IriTech Public Database Results

The (Iris Challenge Evaluation) database contained 20 pairs of iris images generated from IrisAccess. The UUM database is Students with images of varying qualities, including blurry images or images heavily occluded with eyelids, eyelashes, contact lenses, or eyeglasses. Even with this mixture of lower quality images, the result of Iritech's algorithm, when applied to these 20 two-eye pairs, is truly remarkable in that perfect separation--meaning that the FRR and FAR is 0.0000 percent is achieved with no images rejected as show Figure 4.10.

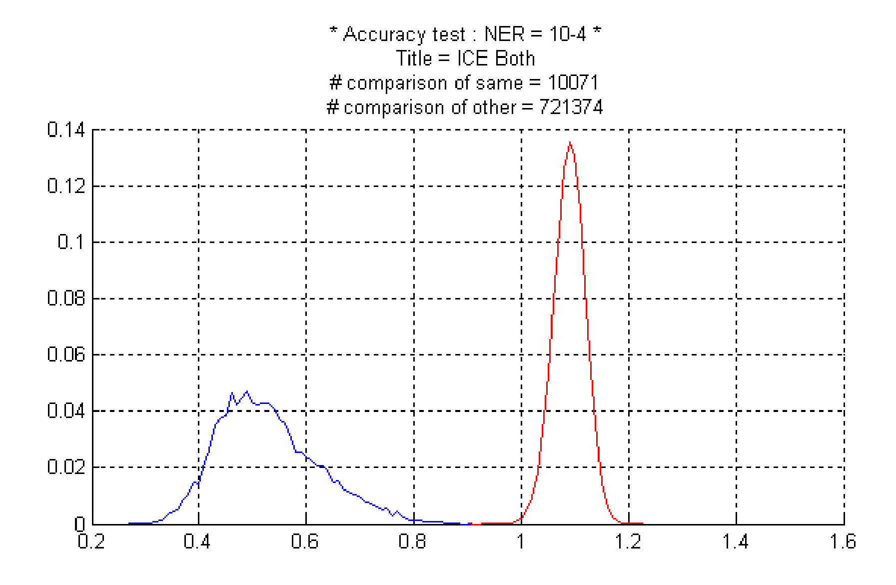



**Figure 4.10:** comparison between FRR and FAR

### 4.10 IRIS Data Base

The public IRIS database contained 20 right, single-eye, images, captured from an Panasonic camera. These images were again heavily occluded, with a variety of different illumination conditions. These adverse image conditions were purposely included to test the resiliency of iris recognition algorithms. Indeed, some images are so poor that the entire iris is occluded. Below is Iritech's result with the IRIS database using two-eye pairs (EER .51%) as show Figure 4.11. and 4.12:

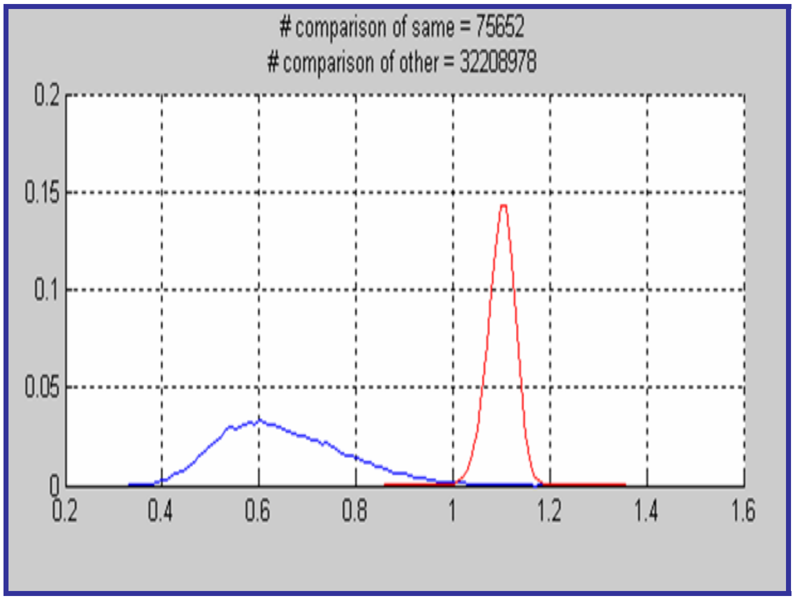



**Figure 4.11:** Images were again heavily occluded.

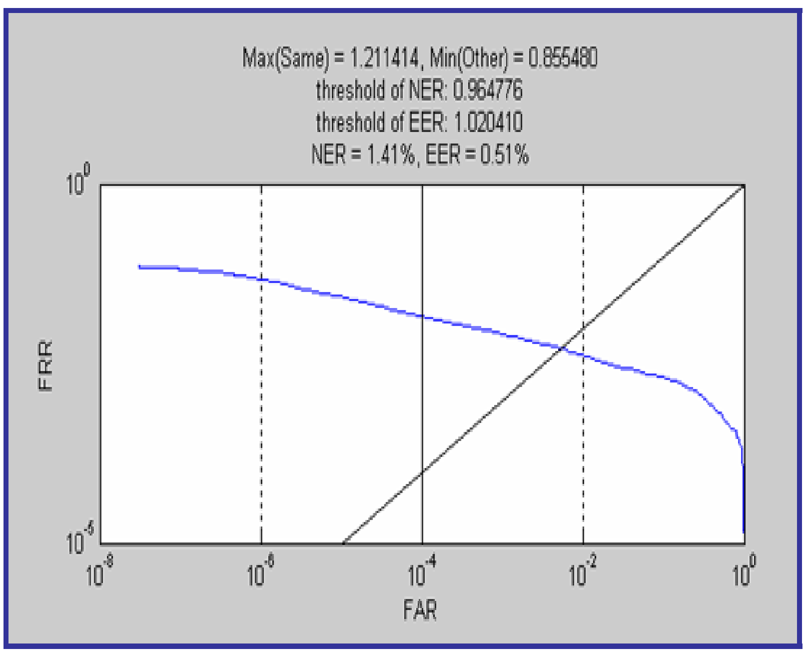



**Figure 4.12:** with a variety of different illumination conditions

**4.11 UBIRIS**

The UBIRIS public database contained 20 images (all of right eye) of very poor quality captured with a Compact camera. Iritech, even with these poor quality color images, only had to reject 4 images to again achieve perfect separation as show Figure 4.13. And 4.14

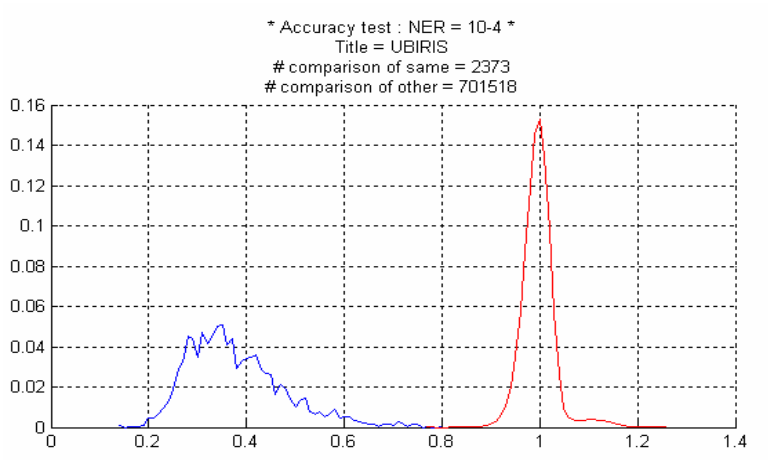



**Figure 4.13:** very poor quality captured

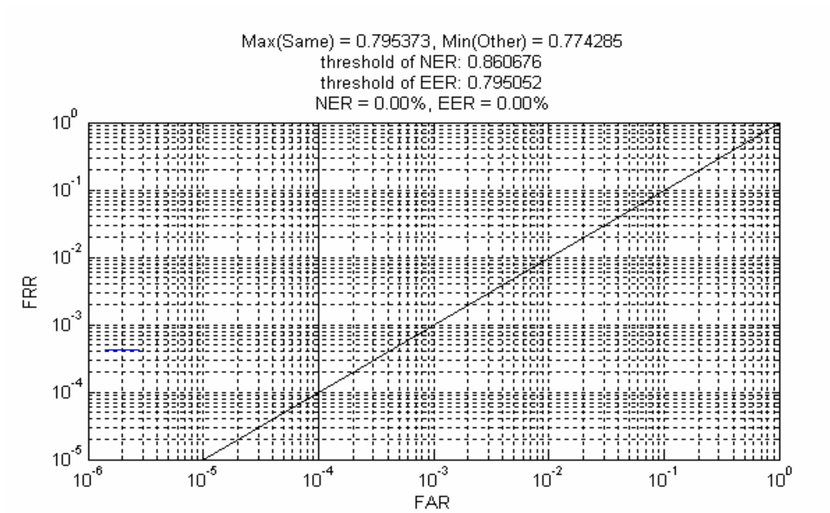



**Figure 4.14:** Reject images.

### 4.12 Conclusion

Iris recognition as a biometric technology has great advantages such as variability, stability and security. Thus it will have a variety of applications. A new and efficient iris recognition algorithm has been implemented, which represents Eigen irises after determining the centre of each iris and finally recognition is based on Euclidean distances. Results have been obtained using four iris images for training purpose; also whenever a new class is added it is necessary to retrain the system. Variations in number of training images affect both the success rate and speed of CPU.

# CHAPTER FIVE

# CONCLUSIONS AND FUTURE WORK

## 5.1 Conclusions

In this work, an iris recognition system has been designed. The system hardware consists of digital video camera and a complete computer system.

The software built program consists of:

1. Image processing for getting an enhancement iris pattern image.
2. Neural network for recognition by utilizing the data of the iris pattern.

The neural network stage consists of two phases:

1. Training phase for human iris identifying and testing phase for deciding whether the human iris exists on the database or not.
2. Methods of neural network have been used in this thesis: LAM method and BPN method.

The NN method using in this work yielded the results can summarized by as below

- Capturing a photo by using windows movie maker program is faster in capturing than hardware digital camera bottom whit start windows.

- NIR light is very important to clarify the details of iris pattern, and the white light is important for constricting the pupil to its narrow size.
- Dealing with JPEG type of pictures proved to be successful.
- Getting the iris location is performed by following the darkness density of pupil.
- Data equalization is obtained by using histogram equalization at the beginning and at the end of image analysis.
- Iris image can be converted to the matrix for STD values instead of pixels intensity. In which STD values attained good results.
- ANN has fast mathematical methods for identification.
- Backpropagation neural network can be used for iris pattern classification.
- Momentum technique with multiple activation function in backpropagation has advantages in speed and accuracy.
- LAM network is a fast way for identification but it has high rate of percentage error compared with the other employed methods.
- Text file which created for storing the databases is very small in size and easy for translating its contents to another computer.
- The iris recognition system designed is general, easy to use, fast and compatible with different computers.
- MATLAB program (version 7.0 or more) provides fast functions for image processing and neural networks.

## 5.2 Future work

There are some ideas for future work and recommendations to improve this research. The following points display the ideas:

- Identification report can be created for each tested person by the system. This report may have: name, job, address, etc.
- Multi-online person's recognitions system can be designed.
- The iris picture can be captured at suitable distance by using high performance camera.
- Iris and retina patterns recognition can be designed and implemented in one combinational system.

# REFERENCES

Amer, R. (2001). "Design a software application for Iris Identification by Artificial Neural Network", M. Sc. Thesis, Computers and Mathematical Sciences College, University of Mosul/ Iraq.

Al-Sumaidaee, H. A. (2005). "Off-Line Handwritten Signature Verification Using Backpropagation Neural Network", M. Sc. Thesis, Technical College, Mosul/Iraq.

Aminzadeh, F. Barhen J. Glover, C. W. and Toomarian, N. B. (2000). Reservoir parameter estimation using hybrid neural network, Computers & Geoscience, vol. 26, pp. 869-875.

Berry, M. J. A. and Linoff, G.(1997). Data Mining Techniques, John Wiley & Sons, Inc.

Burghardt, T.(2000) "Inside Iris Recognition", Master course in global computing and multimedia, university of Bristol, November.

Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, (2006). Performance evaluation of fingerprint verification systems, IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 1, pp. 3–18.

Chang, W. Y (2004). "Image Processing with Wreath Products", M. Sc. Thesis, Harvey Mudd college, Department of Mathematics.

Chang, H. C. Kopaska-Merkel, D. C. Chen, H. C. and Durrans, R. Lithofacies (2000). Identification Using Multiple Adaptive Resonance Theory of Neural Networks and Group Decision Expert System, Computers and Geosciences vol 26, pp.591-601.

Chen H. C. and Fang. J. H. (1993). A new method for prospect appraisal. AAPG Bull., vol. 77, pp. 9-8.

Dory L. Hudspeth, Sarah J. Spinks, (2001). "Iris Scan Technology", Faulkner Information Services, and Publication Date: 0109, Publication Type: TUTORIAL.

Daugman, J. (1993). "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE transactions on pattern analysis and machine intelligence. Vol. 15, No. 11.

Daugman, J. (2004). *"How Iris Recognition Works", IEEE transactions on circuits and systems for video technology*, Vol. 14, No.1.

Daugman, J. Downing, C. (2001). *"Epigenetic randomness, complexity and singularity of human iris patterns",* The Royal Society, Proc. R. Soc. Lond. B 268, 1737-1740.

Daugman, J. (2003). "The importance of being random: statistical principles of iris recognition", The journal of the pattern recognition society, Pattern Recognition 36, 279 – 291.

Dunker, M. (2004). "Don't blink: Iris recognition for biometric identification", SANS institute as part of GIAC practical repository, pp.1-17.

Daugman, J. G. (1993). *"High Confidence Visual Recognition of Persons by a Test of Statistical Independence",* IEEE Trans. Pattern Analysis and Machine Intelligence, vol.15, no.11, pp.1148-1161.

Daugman, J. (1994). Biometric personal identification system based on iris analysis. U.S. Patent No. 5,291,560.

Daugman, J. (2005). Results from 200 billion iris cross-comparisons. Technical Report UCAM-CL-TR-635, University of Cambridge Computer Laboratory, June 2005.

Fausett, L. (1994). *"Fundamental of Neural Networks, Architectures, Algorithms and Applications",* Printice Hall Int.

Hocquet, S. Ramel, J. Cardot, H. (2005). Fusion of Methods for Keystroke Dynamic Authentication, Automatic Identification Advanced Technologies, 2005. Fourth IEEE Workshop Page(s):224 - 229

Istook, E. Martinez, T. (2002). "Improved back propagation learning in neural networks with windowed momentum", International journal of neural systems, vol. 12, no. 3&4, pp. 303-318.

Jain, A. K. (2004). "Biometric recognition: how do I know who you are?" Signal Processing and Communications Applications Conference. Proceedings of the IEEE 12th: 3 - 5

Jain, A. K. Ross, A. & Pankanti, S., (2006). "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security.

Johnson, R. G. (1991). “Can iris patterns be used to identify people?” Chemical and Laser Sciences Division LA-12331-PR, Los Alamos National Laboratory, Los Alamos, Calif.

Kukula, E. Elliott, S. (2005). Implementation of Hand Geometry at Purdue University's Recreational Center: An Analysis of User Perspectives and System Performance, IEEE.

Lim, J. S. (1990). "Two-dimensional signal and image processing", Prentice Hall signal processing series.

Lawton, G. (1998). “Biometrics: A New Era in Security”, IEEE Computer, pp.16-18.

Mohammed, R, A.  Ibrahim, N, B. Nori, A, S. (2004) "Iris Identification Software (IIS)", Raf. Jour. Sci., Vol. 15, No. 1Comp. Math. & Stati. Special Issue, pp. 1-10, Maerivoet, S. (2000). "An introduction to image enhancement in the spatial domain", University of Antwerp, Department of mathematics and computer science.

Omlin, C. W. and Giles, C. L. (2008). Symbolic Knowledge Representation in Recurrent Neural Networks: Insights from Theoretical Models of Computation.

Golden, R. M, (1996). Mathematical Methods for Neural Network Analysis and Design. Cambrigde, MA: MIT Press.

Patina, F (2003). "An introduction to digital image processing", homepage yov408, pp 1-49.

Philips, P. J. Grother, P. R. Micheals, R. Blackburn, D. M. Tabassi, and J. M. (2002). Bone, Face Recognition Vendor Test.

Zhu, Y. Tan, T. Wang, Y (2000). "Biometric Personal Identification Based on Iris Patterns", Proc. Int. Conf. on Pattern Recognition, Vol. 2, pp. 801-804.

Roizenblatt, R. Schor, P. Dante, F. Roizenblatt, J. Belfort, R. (2004). "Iris recognition as a biometric method after cataract surgery", BioMedical Engineering 3:2, pp. 1-7.

Riha, Z. Matyas, V. (2000). "Biometric Authenrication Systems", Faculty of Informatics Masaryk University (FIMU), FIMU-RS.

Rosenzweig, P. Kochems, A. Schwartz, A. (2004). "Biometric Technologies: Security, Legal, and Policy Implications", Published by The Heritage Foundation, Legal Memorandum.

Russ, J. C. (2004). "Seeing the Scientific Image", Proceedings RMS, Vol. 39/2.

Shindala, N. (2004). "Speaker Recognition using neuro-fuzzy method", M. Sc. Thesis, Computer Engineering college, university of Mosul/Iraq, 2004.

Umbaugh, S. E (1998). "Computer vision and image processing: A practical approach using CVIPtools", Prentice Hall PTR.

Fisher, R. Perkins, S. Walker A. and Wolfart, E. (2003). "Laplacian / Laplacian of Gaussian".

Wildes, R. P. (1997). “Iris Recognition: An Emerging Biometric Technology”, Proceedings of the IEEE, vol.85, pp.1348-1363.

Wilson, A. R. Hicklin, H. Korves, B. Ulery, M. Zoepfl, M. Bone, P. Grother, R. J. Micheals, S. Otto, and C. Watson, (2004). Fingerprint vendor technology evaluation 2003: summary of results and analysis report, NIST Internal Rep. 7123.

Wong, P. M. Gedeon, T. D. and Taggart, I. J. (1995). An improved technique in prediction: A neural network approach, IEEE Trans. Geosci. Remote Sensing, vol. 33, pp. 971.

Zhang, D. (2000) “Biometrics Technologies and Applications”, Proc. of International Conference on Image and Graphics, pp.42-49, Tianjing, China.

Zurada, J. M. (2004) Knowledge-Based Neurocomputing, The MIT Press, Massachusetts. p.65,.

Fornell, Claes and Jaesung Cha (2004), “Partial Least Squares,” in Advanced Methods of Marketing Research, Richard P. Bagozzi, ed. Cambridge, MA: Blackwell, 52-78.

Garbarino, Ellen and Mark S. Johnson (1999), "The Different Roles of Satisfaction, Trust, and Commitment in Customer Relationships," Journal of Marketing, 63 (2), 70-87.

Grossman, Randi P. (2008), "Developing and Managing Effective Consumer Relationships," Journal of Product and Brand Management, 7 (1), 27-40.

Gustafsson, Anders and Michael D. Johnson (2004), "Determining Attribute Importance in a Service Satisfaction Model", Journal of Service Research, Volume 7, No. 2, November 2004 124-141.

Hand, D., H. Mannila, and P. Smyth, (2001), Principles of Data Mining. MIT Press, 2001.

Hastie, T., R. Tibshirani and J. Friedman (2001), The Elements of Statistical Learning Data Mining, Inference, and Prediction. Springer.

Hruschka, Harald (2001), An Artificial Neural Net Attraction Model (Annam) To Analyze Market Share Effects Of Marketing Instruments, Schmalenbach Business Review u Vol. 53 u January 2001 u pp. 27 – 40

Hahn, Carsten, Michael D. Johnson, Andreas Herrmann and Frank Huber (2002), "Capturing Customer Heterogeneity Using A Finite Mixture PLS Approach", Schmalenbach Business Review, Vol. 54, July 2002, 243 – 269

Johnson, Michael and Anders Gustafsson (2000), Improving Customer Satisfaction, Loyalty and Profit: An Integrated Measurement and Management System. San Francisco: Jossey-Bass.

Jones, Tim And Shirley, F. Tayler (2003). The Conceptual Domain of Service Loyalty: How Many Dimensions? Unpublished manuscript.

Keiningham, Timothy L. ,Tiffany Perkins-Munn and Heather Evans (2003), "The Impact of Customer Satisfaction on Share Of Wallet in a Business-to-Business Environment", Journal of Service Research, Vol6, No. 1, August, 2003, 37-50

Kumar, Piyush (1998), "A Reference-Dependent Model of Business Customers' Repurchase Intent," working paper,William Marsh Rice University, Houston, TX.

Mittal, Vikas and Patrick M. Baldasare (1996), “Impact Analysis and the Asymmetric Influence of Attribute Performance on Patient Satisfaction,” Journal of Health Care Marketing, 16 (3), 24-31.

Mittal, Vikas and Jerome Katrichis (2000), “Distinctions between New and Loyal Customers,” Marketing Research, 12 (Spring), 27-32.

Mittal, Vikas, William T. Ross, and Patrick M. Baldasare (1998), “The Asymmetric Impact of Negative and Positive Attribute-Level Performance on Overall Satisfaction and Repurchase Intentions,” Journal of Marketing, 62 (January), 33-47.

Oliver, Richard L. (1997), Satisfaction: A Behavioral Perspective on the Consumer. New York: McGraw-Hill.

Oliver, Richard L (1999), "Whence Consumer Loyalty," Journal of Marketing, 63 (Special Issue), 33-44.

Pritchard, Mark P., Mark E. Havitz, and Dennis R. Howard (1999), "Analyzing the commitment-loyalty link in service contexts," Journal of the Academy of Marketing Science, 27 (3), 333-48.

Pugesek, B. H., A. Tomer, A. and A. Von Eye (2003), Structural Equation Modeling: Applications in Ecological and Evolutionary Biology. Cambridge University Press.

Sharma, Neeru and Paul G. Patterson (2000), "Switching costs, alternative attractiveness, and experience as moderators of relationship commitment in professional, consumer services.," International Journal of Service Industry Management, 11 (5), 470-90.

Reichheld, Frederick (1996). The Loyalty Effect: The Hidden Source Behind Growth, Profits, and Lasting Value. Boston: Harvard Business School Press.

# APPENDIX A

### A.1 How to use iris recognition

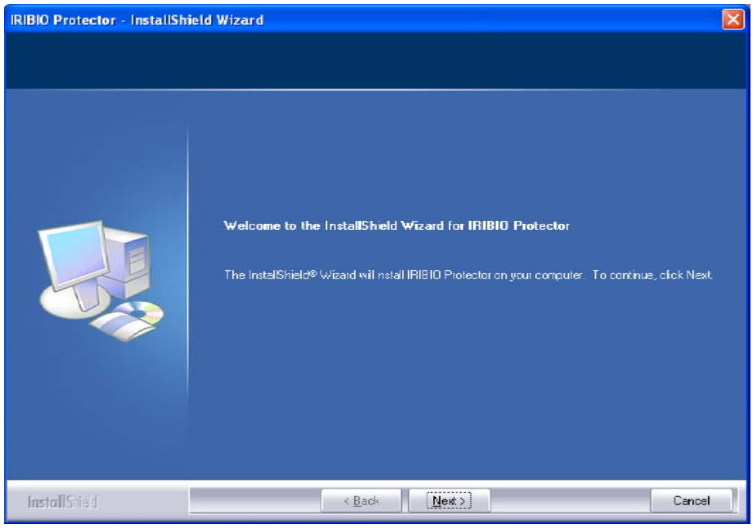
Before you proceed with installation of the program.The Iris camera system is located on the left side of the iris Mouse. It is the mirror to capture an Iris image of a person; the system should have iris guidance for a person to place his eye at right position.

a. Hold your iris mouse as illustrated on page 2, and bring it to your iris as close as 3~5 cm.
b. Look at the mirror and move forward and backward to get your reflected image clear for the best focus. When you move forward and backward, you can observe that the farther you move the mouse away, the more out focused your reflected image become, or vice versa. Try to get to the point where you think your reflected iris image is best focused.
c. You have learned how to use the Iris recognition system. Try to do the same thing when you are required to recognize yourself with Iris Camera.
d. The actual registration, the white LED will be lighted on from lighter degree to the brightest one. The purpose of illuminating the iris is to force your pupil to contract. Please do not be surprised when the white light is turned on. This will only take place when registering except for recognizing in the dark environment.

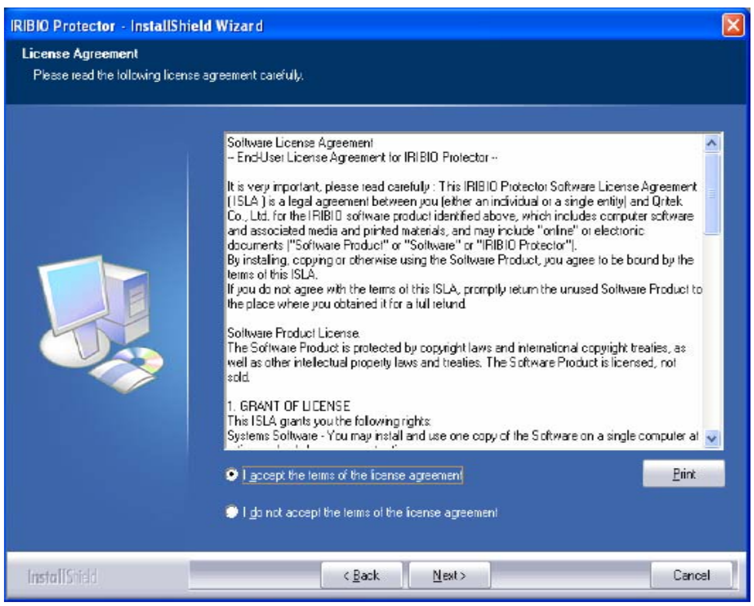
### A.2 Installing Iris recognition Protector

You are now ready to install Iris recognition Protector Software. Before you install,

1. Go to CD drive, and find "IRIS PROTECTOR_ENGLISH.EXE" file to begin installation process. After the location of the installation file, double click it.

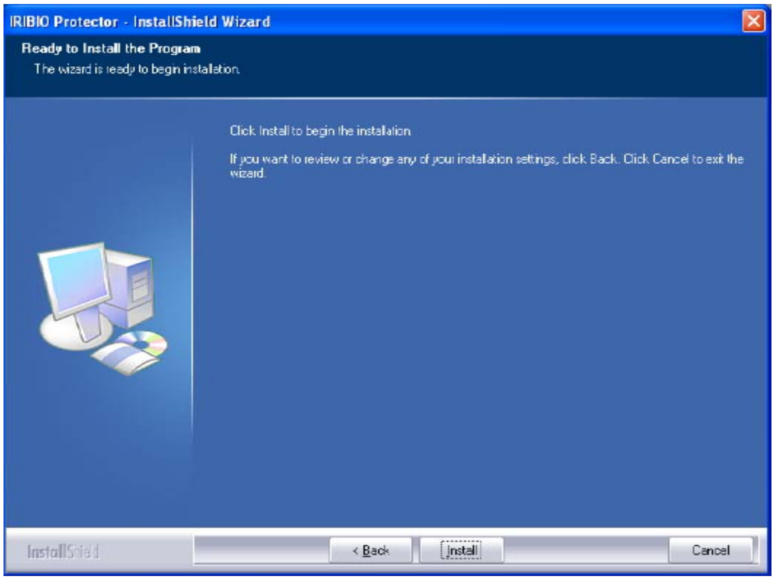



2. Click "Next" button to continue installation.

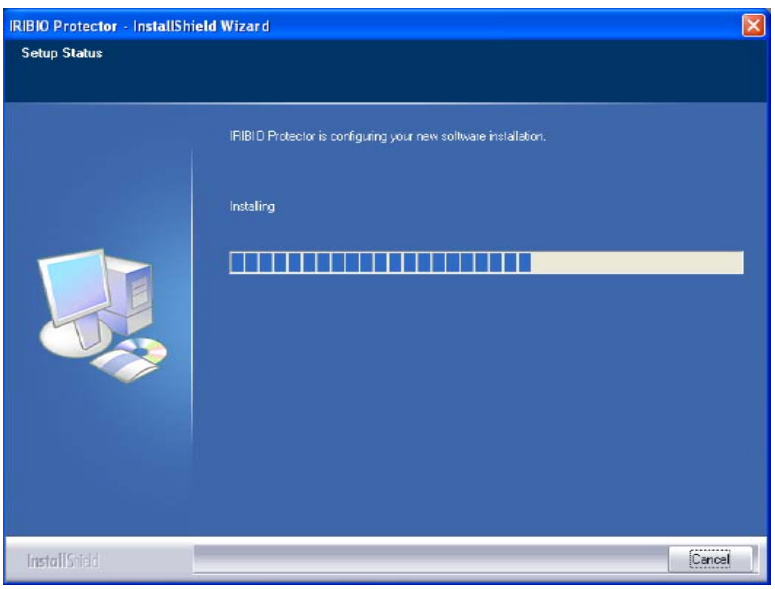



3. Select "I accept." if you agree with the terms and conditions. If not, click "Cancel" to exit the installation program.

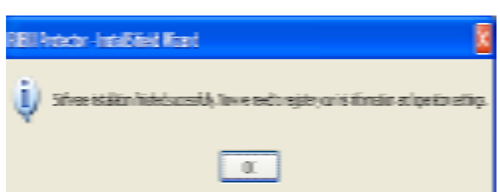
4. After selecting "I accept agreement. "click "Next" to continue installation.



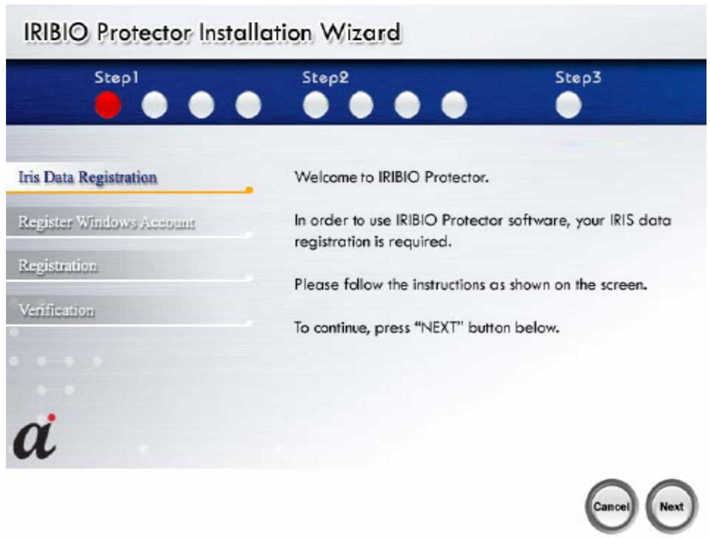

5. Click "Install" button to go into the process of installation.



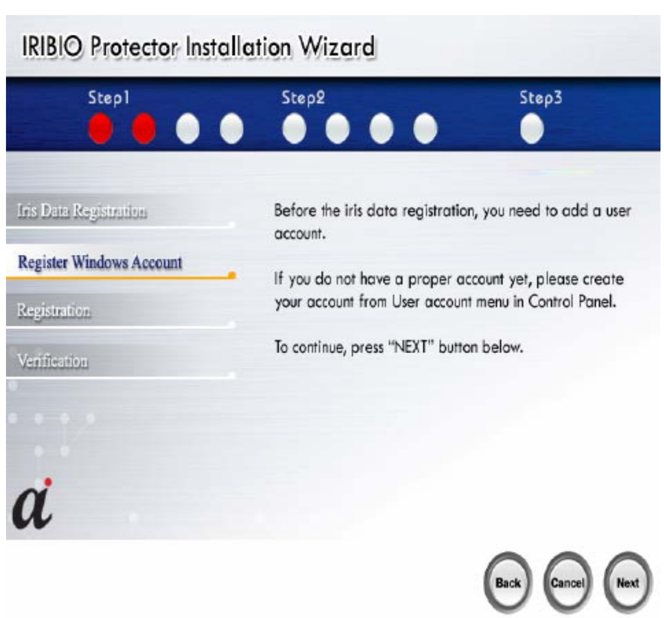

6. You are required to wait until the following message appears on the screen.



This means that the required program files are copied to the computer successfully, and need to register your iris data into the computer as per the normal procedures as shown below.




With this screen, you can now start registering your iris data into your computer. Carefully read the guides on the screen, and click "Next" button to proceed further.

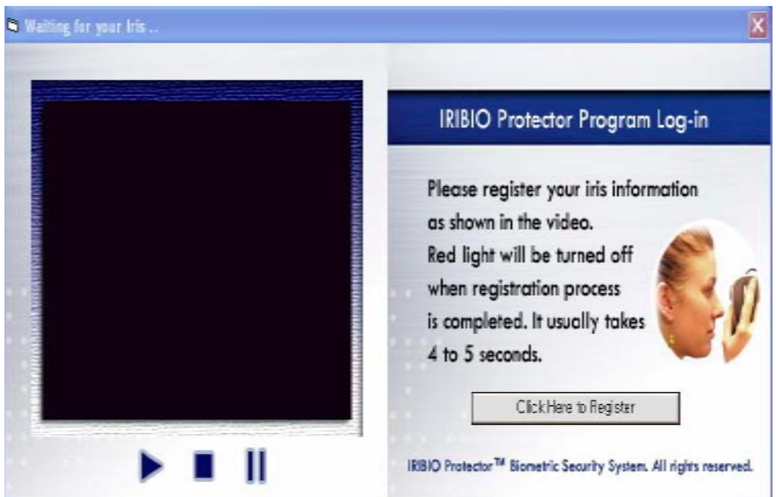


Iris recognition Protector Program requires Windows User Account. If you do not have proper Windows account information, please create Windows User Account in control panel, of which account shall have User Account as well as User password. Clicking “Next” will bring the next screen.


• Add User

- User Account : One of Windows User Account shall be used. User account shall have Computer Administrator right. Hence the restricted user account can not be used.
- Password: A password of Windows User Account shall be used.
- Emergency Password

After registering Windows Account, you will see the above screen. Clicking "Next" button will ask you to register your iris data.




A video guide is being played in left screen, which is helpful for the first user to understand how to register his iris data after seeing it, you can now start iris data register by clicking "Click here to register".

Once you click the button, then RED (IR) lamp attached on the concave mirror of the iris camera will be ON. Then you have to look at the mirror with the distance from 3 to 4 cm, so that your iris image can be clearly shown on the mirror surface. A white LED will be ON with some steps (OFF - light ON – lighter ON – light ON – OFF) for acknowledging your iris changes in response to the light condition. If the registering process is done successfully, a message will be shown.


Click "OK" button and repeat the same in order to register your iris data correctly. If the 2nd registering step is also done completely, then the following message will be shown. This means that iris data registration is complete. Clicking "OK" button will bring the next screen to go ahead further

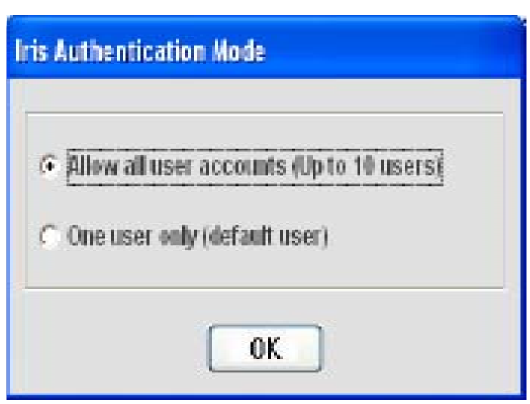

In order to verify that your registered data is fine, you are required to verify your iris data before the next stapes to go. Click "Next" button.


Click the button "Click here to authenticate", and look at the iris mouse mirror in the same manner as you are registering iris data. If your iris is identified successfully, then the following message will appear.

Clicking "OK" button will bring the next screen for further steps

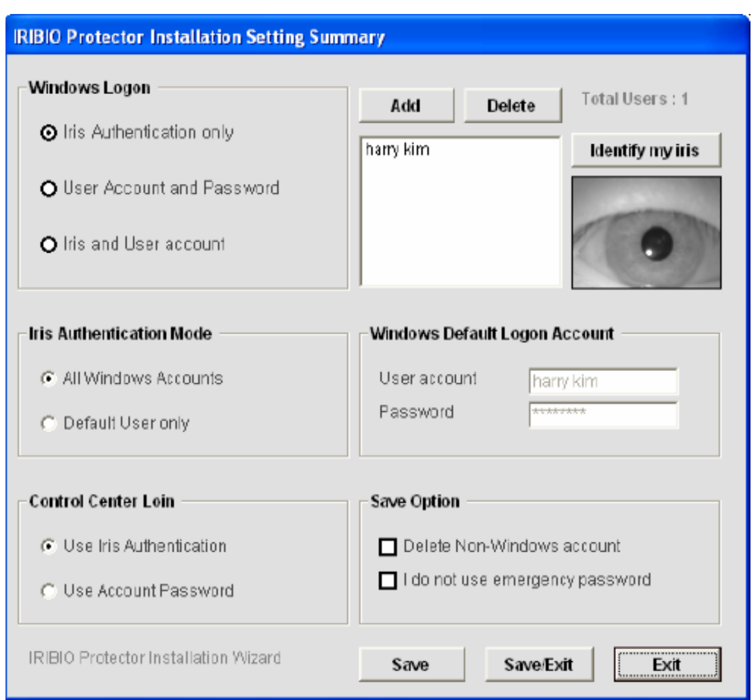
Iris authentication when PC booting or recovering the screen after screen saving, you will be requested to authenticate with your iris.


When using iris authentication for Windows Logon modes explained before, you will also have a option to select who can logon Windows system when computer booting.

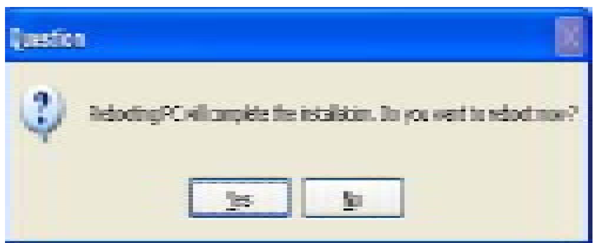


1. Allow all user accounts. If any of Windows account users are verified with his iris, Windows system will be logged on.

2. One user only (Default User)

Carefully review all settings you have chosen during installation process, and save the settings before exit. If you want to add the more users' iris data, then you can use "ADD" button in the screen, and follow the instructions thereafter.




This is final step for installation. Clicking "Yes" will reboot PC for reconfiguration of the system

**A.3 Windows Log-On method**

When the PC is rebooting, after installation, you will see the following screen.

Pressing Ctrl + Alt + Del key combination at a same time will bring you to the next screen as per your Windows Log-on mode setting which was done when program installation process. 3

In case your Windows Log-on mode is iris authentication


Ress the button and get authentication from the system with your iris mouse to log-on. Failure to get a valid authentication will freeze the Window system, and you can not use your computer until a valid iris authentication.

Even though you have selected iris authentication mode for Windows Log-on mode, you may not use your iris mouse due to its trouble or mouse missing. In this case you will see the alternative screen, which is emergency password logon, if you have not set emergency password usage disable mode.