IRIS RECOGNITION TECHNOLOGY

SEMINAR REPORT

Submitted by

ANJUMOL K PRASAD

S2 MCA

Reg. No. 2103

DEPARTMENT OF COMPUTER APPLICATIONS
COLLEGE OF ENGINEERING
THIRUVANANTHAPURAM

December 2008

ABSTRACT

The term "biometrics" is derived from the Greek words bio (life) and metric (to measure). Biometrics is the science of measuring and statistically analyzing biological data. In information technology, biometrics refers to the use of a person's biological characteristics for personal identification and authentication. Fingerprint, iris-scan, retinal-scan, voiceprint, signature, handprint and facial features are some of the most common types of human biometrics.

Iris recognition is a method of biometric authentication that uses pattern recognition techniques based on high-resolution images of the irises of an individual's eyes. Iris recognition uses camera technology, with subtle IR illumination reducing specular reflection from the convex cornea, to create images of the detail-rich, intricate structures of the iris. Converted into digital templates, these images provide mathematical representations of the iris that yield unambiguous positive identification of an individual.

CONTENTS

ACKNOWLEDGEMENT

First of all, I am grateful to **God Almighty**, for helping me to do a seminar on this topic. Without His blessings, I would not have been able to complete this seminar.

I hereby express my gratitude to my guides **Vinod Chandra S.S.** and **John Prakash Joseph**, Lecturers of Department of Computer applications, College of Engineering Trivandrum, for their valuable guidance, constant encouragement and creative suggestions during the course of this project work, and also in preparing this report. I also express my thanks to **Prof. Reji John,** Head of the Department, Department of Computer applications, College of Engineering Trivandrum for all necessary help extended by her in the fulfillment of this project work. I am also grateful to my family, all my friends and classmates for their help and support during the preparation and presentation of this paper.

Anjumol K Prasad

1. INTRODUCTION

Imagine how convenient it would be to activate the security alarm at your home with the touch of a finger, or to enter your home by just placing your hand on the door handle. How would you like to walk up to a nearby ATM which will scan your iris so you can withdraw money without ever inserting a card or entering a PIN. You will basically be able to gain access to everything you are authorized to, by presenting yourself as your identity.

This scenario might not be as far off as we might expect. In the near future, we may no longer use passwords and PIN numbers to authenticate ourselves. These methods have proven to be in secure and unsafe time and time again. Technology has introduced a much smarter solution to us: Biometrics.

Biometric authentication will help in enhancing the security infrastructure against some of these threats. After all, physical characteristics are not something that can be lost, forgotten or passed from one person to another. They are extremely hard to forge and a would-be criminal would think twice before committing a crime involving biometrics.

2. BIOMETRICS SYSTEM

The four basic elements of a typical biometric system are: sensing, processing, storage and interface to an existing infrastructure.

2.1 ABOUT BIOMETRICS

Biometrics is automated methods of recognizing a person based on a physiological or behavioural characteristic. The word biometrics means Biological Measurements. Therefore in this way we can use computers to recognize persons.

- Physiological characteristics means Fingerprints, Retinal and Iris Patterns, Hand and Finger Geometry, Facial recognition etc.
- Behavioral characteristics mean Voice Patterns, Signature etc.

There are different biometric solutions. Some of them are Finger Print Recognition, Iris Pattern recognition, Facial Recognition; Voice Pattern

Recognition, Hand and Finger Geometry etc. In all these biometric solutions the details about the physiological/behavioral characteristics are entered into a database. When the user uses the system the characteristics required for the system are scanned and a template is formed. It is checked whether there exists a match for this template with any of the records already stored in the database. If a match is found, the user is allowed access. Otherwise the user is denied access.

Each biometric solution can be used in two different modes.

- In Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match.
- In Verification mode, where the biometric system authenticates a person's claimed identity from his/her previously enrolled pattern.

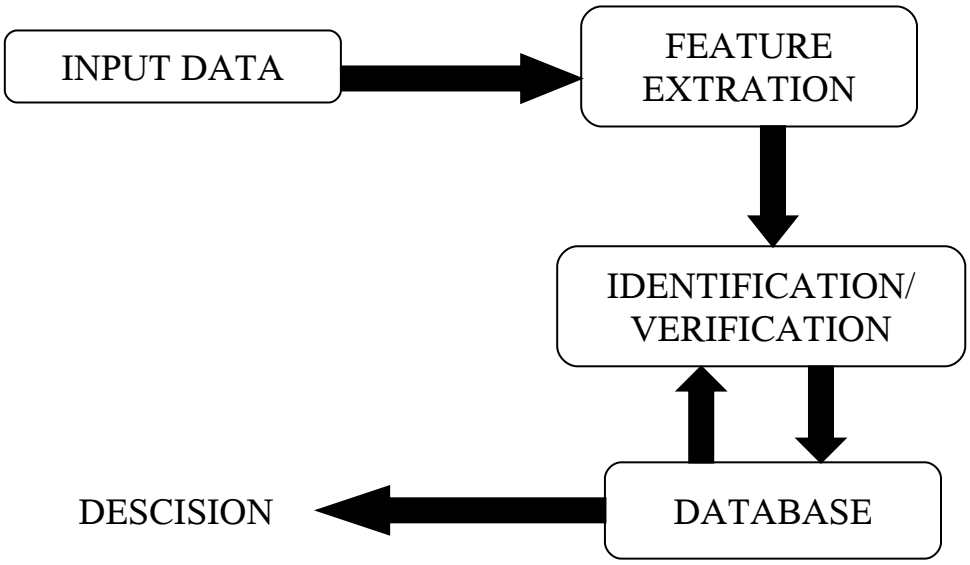


Figure 1.1 Basic Biometric Authentication Systems

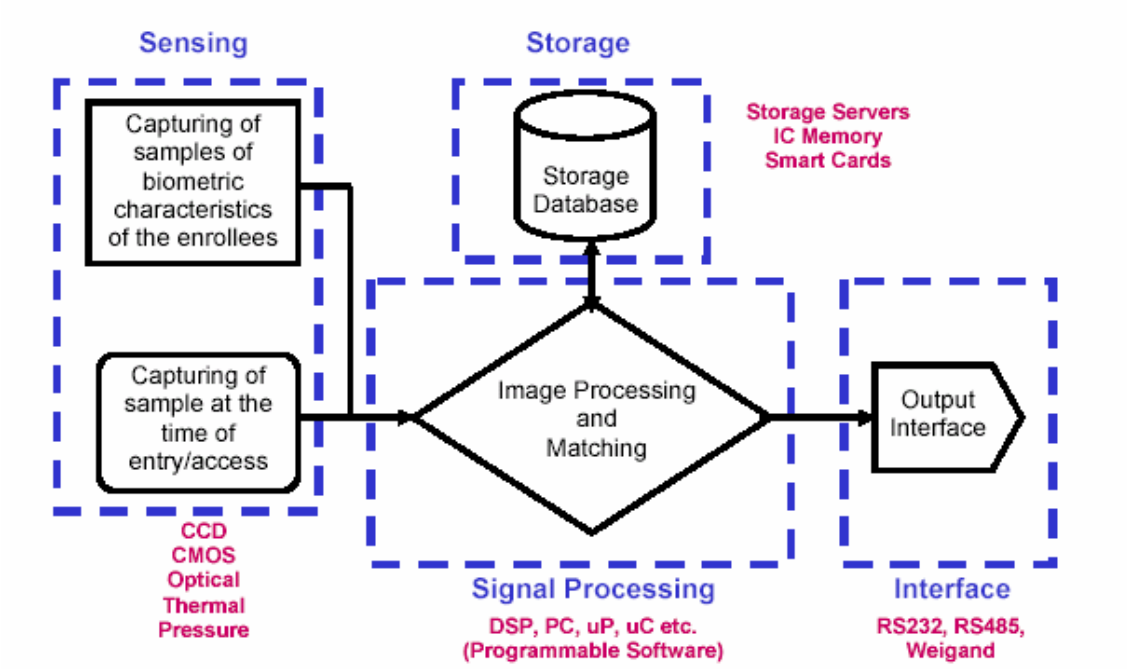


Figure 2. Biometrics System Elements

2.2 SENSING ELEMENT

The sensing element, or the input interface element, is the hardware core of a biometrics system and converts human biological data into digital form. This could be a complimentary metal oxide semiconductor (CMOS) imager or a charge coupled device (CCD) in the case of face recognition , handprint recognition or iris/retinal recognition systems; a CMOS or optical sensor in the case of fingerprint systems; or a microphone in the case of voice recognition systems.

The following are notes on the biometric sensing.

- Finger Print Recognition.
- Iris Recognition.
- Facial Recognition.

The validity of a biometric system cannot be measured accurately, and can only be enumerated on the occurrence of errors like the chance of accepting an intruder i.e. the False Accept Rate (FAR) and conversely the probability of

rejecting a genuine individual i.e. False Reject Rate (FRR) which could turn out to be detrimental to any system.

2.3 TYPES OF BIOMETRICS

2.3.1 Bertillonage,

The first type of biometrics came into form in 1890, created by an anthropologist named Alphonse Bertillon. He based his system on the claim that measurement of adult bones does not change after the age of 20. The method consisted of identifying people by taking various body measurements like a person's height, arm length, length and breadth of the head, the length of different fingers, the length of forearms, etc. using calipers. However, the methodology was unreliable as non-unique measurements allowed multiple people to have same results, decreasing the accuracy and hence is no longer used.

2.3.2 Fingerprint Recognition

It involves taking an image of a person's fingertips and records its characteristics like whorls, arches, and loops along with the patterns of ridges, furrows, and minutiae. Fingerprint matching can be achieved in three ways

- Minutae based matching stores minutiae as a set of points in a plane and the points are matched in the template and the input minutiae.
- Correlation based matching superimposes two fingerprint images and correlation between corresponding pixels is computed.
- Ridge feature based matching is an advanced method that captures ridges, as minutiae capturing are difficult in low quality fingerprint images.

To capture the fingerprints, current techniques employ *optical sensors* that use a CCD or CMOS image sensor; *solid state sensors* that work on the transducer technology using capacitive, thermal, electric field or piezoelectric sensors; or *ultrasound sensors* that works on echography in which the sensor sends acoustic signals through the transmitter toward the finger and captures the echo signals with the receiver.

Fingerprint scanning is very stable and reliable. It secures entry devices for building door locks and computer network accesses are becoming more common. Recently a small number of banks have begun using fingerprint readers for authorization at ATMs.

2.3.3 Face recognition

This technique records face images through a digital video camera and analyses facial characteristics like the distance between eyes, nose, mouth, and jaw edges. These measurements are broken into facial planes and retained in a database, further used for comparison. Face recognition can be done in two ways:

• Face appearance employs Fourier transformation of the face image into its fundamental frequencies and formation of *eigenfaces,* consisting of eigen vectors of the covariance matrix of a set of training images. The distinctiveness of the face is captured without being oversensitive to noise such as lighting variations.

• Face geometry models a human face created in terms of particular facial features like eyes, mouth, etc. and layout of geometry of these features is computed. Face recognition is then a matter of matching constellations.

Another face identification technology, Facial thermograms, uses infrared heat scans to identify facial characteristics. This non-intrusive technique is light-independent and not vulnerable to disguises. Even plastic surgery, cannot hinder the technique. This technique delivers enhanced accuracy, speed and reliability with minimal storage requirements. To prevent a fake face or mold from faking out the system, many systems now require the user to smile, blink, or otherwise move in a way that is human before verifying. This technique is gaining support as a potential tool for averting terrorism, law enforcement areas and also in networks and automated bank tellers.

2.3.4 Voice Recognition

It combines physiological and behavioral factors to produce speech patterns that can be captured by speech processing technology. Inherent properties of the speaker like fundamental frequency, nasal tone, cadence, inflection, etc. are used for speech authentication.

Voice recognition techniques can be divided into categories depending on the type of authentication domain.

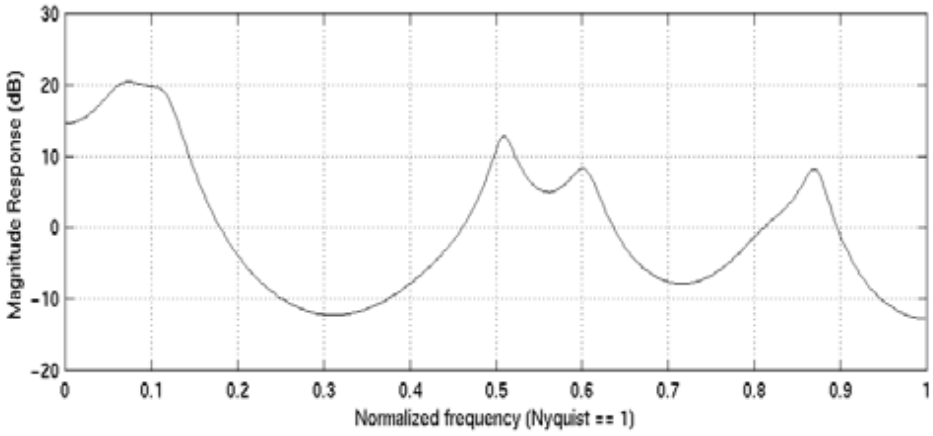
• Fixed text method is a technique where the speaker is required to say a predetermined word that is recorded during registration on the system.

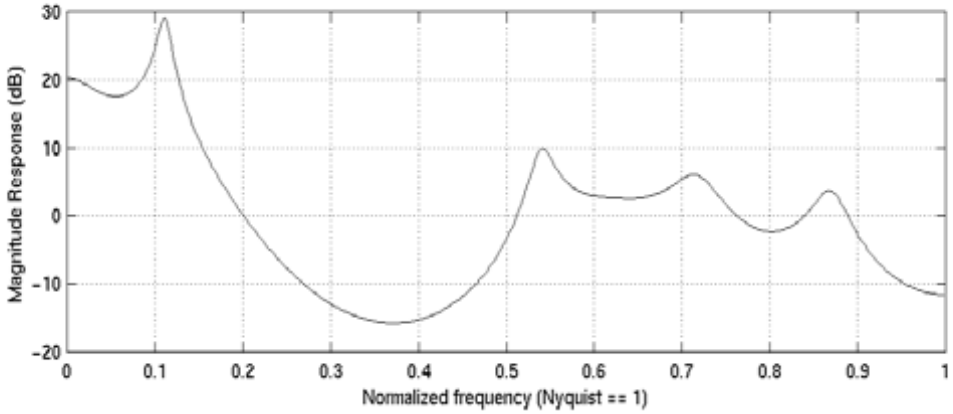
• In the text dependent method the system prompts the user to say a specific word or phrase, which is then computed on the basis of the user's fundamental voice pattern.

• The text independent method is an advanced technique where the user need not articulate any specific word or phrase. The matching is done by the system on the basis of the fundamental voice patterns irrespective of the language and the text used.

• Conversational technique verifies identity of the speaker by inquiring about the knowledge that is secret or unlikely to be known or guessed by a sham.

This interactive authentication protocol is more accurate as the FAR are claimed to be below 10^{-12}.





Illustrates the differences in the models for two speakers saying the same vowel.

Figure 1.3

The vocal-tract is represented in a parametric form as the transfer function H(z). Ideally, the transfer function should contain poles as well as zeros. However, if only the voiced regions of speech are used then an all-pole model for H(z) is sufficient. Furthermore, linear prediction analysis can be used to efficiently estimate the parameters of an all-pole model. Finally, it can also be noted that the all-pole model is the minimum-phase part of the true model and has an identical magnitude spectra, which contains the bulk of the speaker-dependent information.

This technique is inexpensive but is sensitive to background noise and it can be duplicated. Also, it is not always reliable as voice is subject to change during bouts of illness, hoarseness, or other common throat problems. Applications of this technique include voice-controlled computer system, telephone banking, m-commerce and audio and video indexing.

2.3.5 Iris recognition

It analyzes features like rings, furrows, and freckles existing in the colored tissue surrounding the pupil. The scans use a regular video camera and works through glasses and contact lenses. The image of the iris can be directly taken by making the user position his eye within the field of a single narrow-angle camera. This is done by observing a visual feedback via a mirror. The isolated iris pattern obtained is then demodulated to extract its phase information.

Iris image acquisition can be done in two ways:

• Daugman *System* that uses an LED based point light source in conjuction with a standard video camera. The system captures images with the iris diameter typically between 100-200 pixels from a distance of 15-46 cm using 330mm lens.

• Wildes *System* in comparison results in an illumination rig that is more complex. The system images the iris with approximately 256 pixels across the diameter from 20cm using an 80mm lens.

Iris recognition was piloted in Saudi Arabia as a method of keeping track of the millions making Haj. Also it is used a Berkshire County jail for prisoner identification and Frankfurt airport for passenger registration.

2.3.6 Hand geometry

As the name suggests, involves the measurement and analysis of the human hand. Features like length and width of the fingers, aspect ratio of the palm or fingers, width of the palm, thickness of the palm, etc are computed. The user places the palm on a metal surface, which has guidance pegs on it to properly align the palm, so that the device can read the hand attributes.

The basic procedure involves capturing top and side views of the hand using a single camera by judicious placement of a single 45° mirror. To enroll a person in a database, two snapshots of the hand are taken and the average of resulting feature vectors is computed and stored.

Hand Geometry is employed at locations like the Colombian legislatures, San Francisco International Airport, day care centers, a sperm bank, welfare agencies, hospitals, and immigration facilities.

2.3.7 Hand Vascular Pattern Identification

It uses a non-harmful near infrared light to produce an image of one's vein pattern in their face, wrist, or hand, as veins are relatively stable through one's life. It is a non-invasive, computerized comparison of shape and size of subcutaneous blood vessel structures in the back of a hand. The vein "tree" pattern, picked up by a video camera, is sufficiently idiosyncratic to function as a personal code that is extremely difficult to duplicate or discover. The sensor requires no

physical contact, providing excellent convenience and no performance degradation even with scars or hand contamination. Verification speed of the system is fast (0.4 sec/person) and the False Acceptance Rate is FAR) and False Rejection Rate (FRR) are extremely low at 0.0001 % and 0.1% respectively. Though minimally used at the moment, vascular pattern scanners can be found in testing at major military installations and is being considered by some established companies in the security industry and multi-outlet retailers.

2.3.8 Retina Recognition

This technology uses infrared scanning and compares images of the blood vessels in the back of the eye, the choroidal vasculature. The eye's inherent isolation and protection from the external environment as an internal organ of the body is a benefit. Retina scan is used in high-end security applications like military installations and power plants.

2.3.9 Signature recognition

It is an instance of writer recognition, which has been accepted as irrefutable evidence in courts of laws. The way a person signs his name is known to be a characteristic of that individual. Approach to signature verification is based on features like *number of interior contour*s and *number of vertical slope components*. Signatures are behavioral biometric that can change with time, influenced by physical and emotional conditions of the signatories.

Furthermore, professional forgers can reproduce signatures to fool an unskilled eye and hence is not the preferred choice.

2.3.10 DNA Recognition

It employs Deoxyribo Nucleic Acid, which is the one-dimensional ultimate unique code for ones individuality, except for the fact that identical twins have identical DNA patterns. [2] However, it is currently used mostly used in the context of forensic applications. The basis of DNA identification is the comparison of alleles of DNA sequences found at loci in nuclear genetic material.

Method	Coded Pattern	Misidentification rate	Security	Applications
Iris recognition	Iris pattern	1/1,200,000	High	High-security facility
Finger printing	Finger prints	1/1,000	Medium	Universal
Hand shape	Size, length and thickness of hands	1/700	Low	Low-security facility
Facial recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-security facility
Signature	Shape of letter, writing order, pen pressure	1/100	Low	Low-security facility
Voice printing	Voice characteristics	1/30	Low	Telephone service

3. Iris Recognition Technology

The area of human eye where the pigmented or the coloured circle, usually brown or blue, rings the dark pupil of the eye is called the Iris. The human iris begins to form in the third month of gestation and the structure is complete by the eight month, even though the color and pigmentation continue to build through the first year of birth. After that, the structure of the iris remains stable throughout a person's life, except for direct physical damage or changes caused by eye surgery. The iris hence parallels the fingerprint in uniqueness but enjoys a further advantage that it is an internal organ and less susceptible to damages over a person's lifetime. It is composed of several layers which gives it its unique appearance. This uniqueness is visually apparent when looking at its rich and small details seen in high resolution camera images under proper focus and illumination. The iris is the ring-shape structure that encircles the pupil, the dark centered portion of the eye, and stretches radially to the sclera, the white portion of the eye see it shares high-contrast boundaries with the pupil but less-contrast boundaries with the sclera.

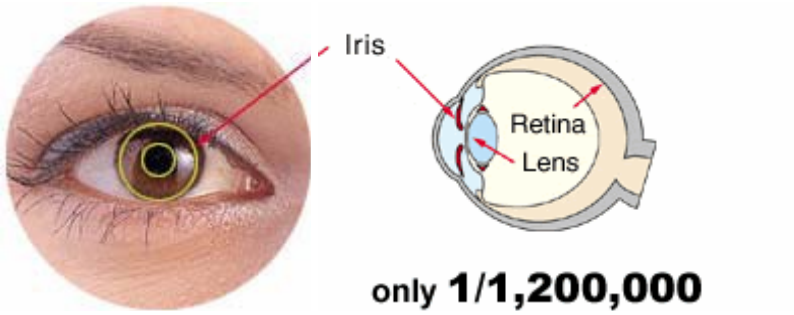


Figure 1.4

The iris identification system is to automatically recognize the identity of a person from a new image by comparing it to the human iris patterns annotated with identity in a stored database. A general iris recognition system is composed of four steps. Firstly, an image containing the user's eye is captured by the system. Then, the image is preprocessed to normalize the scale and illumination of the iris and localize the iris in the image. Thirdly, features representing the iris patterns are extracted. Finally, decision is made by means of matching. There are four key parts the iris recognition system: iris image acquisition, preprocessing, feature extraction, and classifier design.

In a world where we will increasingly do business with parties we've never met, and might never meet, authentication will become as integral a part of the transaction as the exchange of goods and tender. The robustness of iris recognition makes it ideal for authenticating parties to commercial transactions, to reduce fraud in applications like check-cashing and ATMs, unauthorized activity in applications like treasury management, and in future, to ensure non-repudiation of sales, or to provide Letter of Credit and other authentication services in an electronic commerce environment. Daugman has shown that iris patterns have about 250 degrees of freedom, i.e. the probability of two eyes having the same iris texture is about 1 in 7 billion. Even the 2 irises of an individual are different thereby suggesting that iris textures are independent of the genetic constitution of an individual. Iris recognition has been successfully deployed in many large scale and small scale applications.

3.1 IRIS RECOGNITION PROCESS

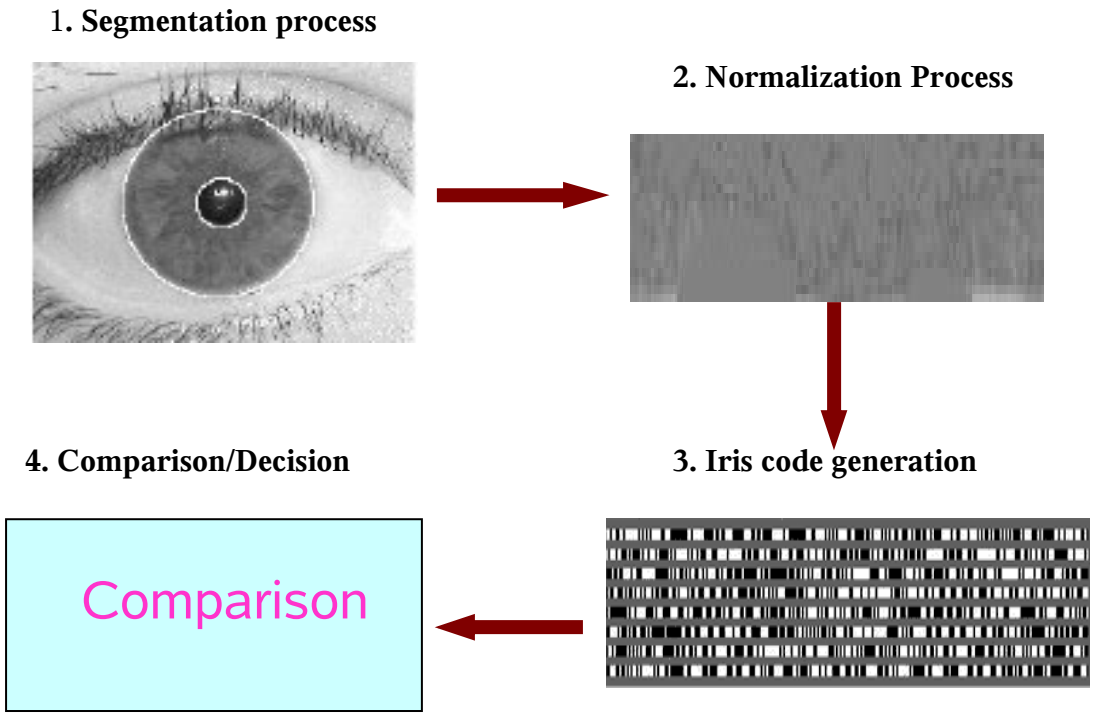


Figure 1.5

3.2 OPERATING PRINCIPLE

An iris-recognition algorithm first has to identify the approximately concentric circular outer boundaries of the iris and the pupil in a photo of an eye. The set of pixels covering only the iris is then transformed into a bit pattern that preserves the information that is essential for a statistically meaningful comparison between two iris images. The mathematical methods used resemble those of modern lossy compression algorithms for photographic images. In the case of Daugman's algorithms, a Gabor wavelet transform is used in order to extract the spatial frequency range that contains a good best signal-to-noise ratio considering the focus quality of available cameras. The result is a set of complex numbers that carry local amplitude and phase information for the iris image. In Daugman's algorithms, all amplitude information is discarded, and the resulting 2048 bits that represent an iris consist only of the complex sign bits of the Gabor-domain representation of the iris image. Discarding the amplitude information ensures that the template remains largely unaffected by changes in illumination and virtually negligibly by iris color, which

contributes significantly to the long-term stability of the biometric template. To authenticate via identification (one-to many template matching) or verification (one-to one template matching) a template created by imaging the iris, is compared to a stored value template in a database. If the Hamming distance is below the decision threshold, a positive identification has effectively been made.

A practical problem of iris recognition is that the iris is usually partially covered by eye lids and eyelashes. In order to reduce the false-reject risk in such cases, additional algorithms are needed to identify the locations of eye lids and eyelashes, and exclude the bits in the resulting code from the comparison operation.

Iris localization is considered the most difficult part in iris identification algorithms because it defines the inner and outer boundaries of iris region used for feature analysis. The main objective here is to remove any non-useful information, namely the pupil segment and the part outside the iris (sclera, eyelids, skin). R. Wildes used Hough transforms to detect the iris contour. Daugman proposed an integro-differential operator to find both the pupil and the iris contour. Daugman's algorithm is claimed to be the most efficient one. After analyzing The Daugman's iris locating and pointing out the some limitations of this algorithm, this paper proposes optimized Daugman's algorithms for iris localization.

3.2.1 Daugman's Algorithm:

Daugman's algorithm is based on applying an integro-differential operator to find the iris and pupil contour.

$$\max(r, x_o, y_o)\left|G_\sigma(r) * \frac{\partial}{\partial r}\oint_{r,x_o,y_o}\frac{I(x,y)}{2\pi r}ds\right|$$

Equation 1. Daugman's Integro-Differential Equation

Where X_0, Y_0, r_o : the center and radius of coarse circle (for each of pupil and iris). $G_\sigma(r)$: Gaussia function. Δr : the radius range for searching for. I(X, Y) : the original iris image.

$G_\sigma(r)$ is a smoothing function, the smoothed image is then scanned for a circle that has a maximum gradient change, which indicates an edge. The above algorithm is done twice, first to get the iris contour then to get the pupil contour. It worth

mentioning here the problem is that the illumination inside the pupil is a perfect circle with very high intensity level (nearly pure white). Therefore, we have a problem of sticking to the illumination as the max gradient circle. So a minimum pupil radius should be set. Another issue here is in determining the pupil boundary the maximum change should occur at the edge between the very dark pupil and the iris, which is relatively darker than the bright spots of the illumination. Hence, while scanning the image one should take care that a very bright spot value could deceive the operator and can result in a maximum gradient. This simply means failure to localize the pupil. The following experimental results have been getting using UPOL database.

3.2.2 Optimized Daugman's Algorithm:

As a solution to this problem, modification to the integro-differential operator is proposed to ignore all circles if any pixel on this circle has a value higher than a certain threshold. This threshold is determined to be 200 for the grayscale image. This ensures that only the bright spots – values usually higher than 245 – will be cancelled.

Another solution we considered is to treat the illumination by truncating pixels higher than a certain threshold – bright spots – to black. But this method failed in many images, this is because when the spot hits the pupil the illumination spreads on the pupil so as we treat the illumination spots it will leave behind a maximum change edges that can not be determined and the operator will consider it the pupil boundary. The sequence of the Algorithm procedure is cleared in the flowchart shown below.

The false acceptance rate for the iris recognition system is 1 in 1.2 million, statistically better than the average fingerprint recognition system. The real benefit is in the false rejection rate, a measure of authenticated users who are rejected.

Fingerprint scanners have a three percent false rejection rate, whereas iris scanning systems boast rate at the 0% level.

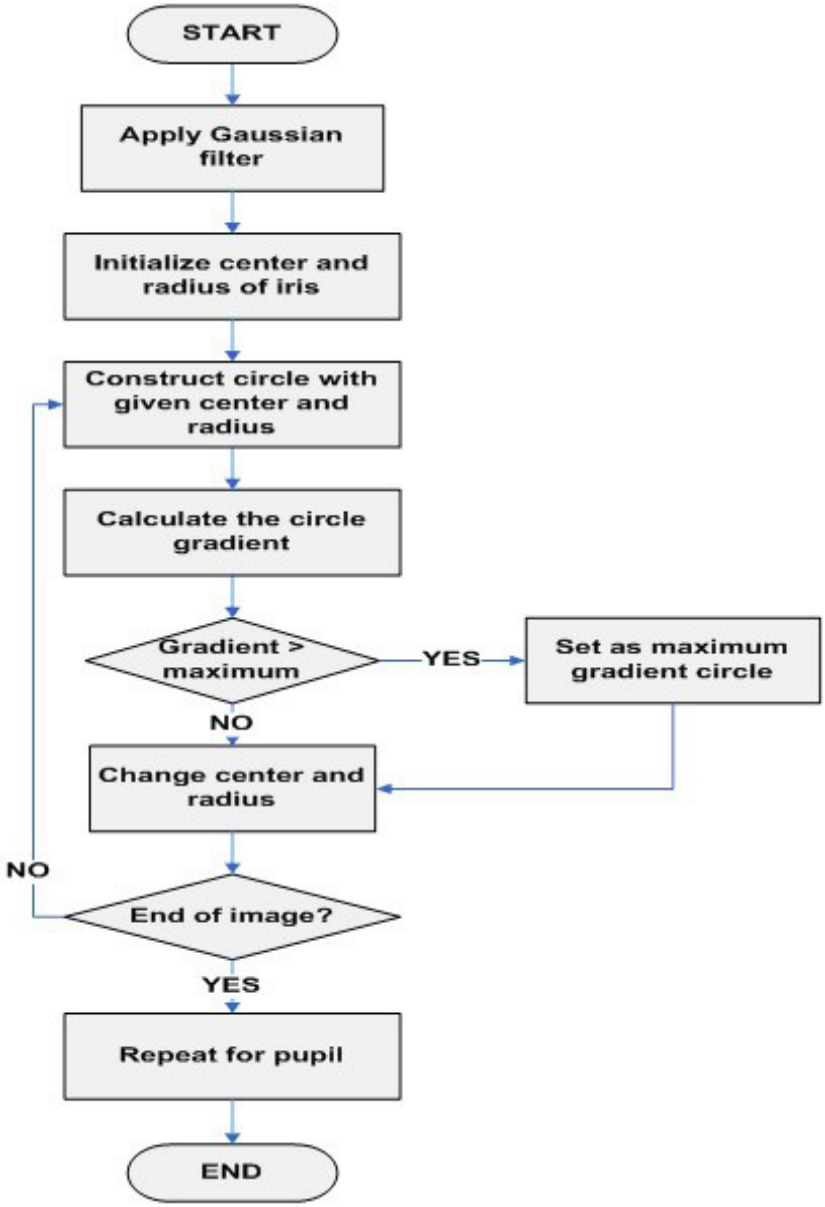
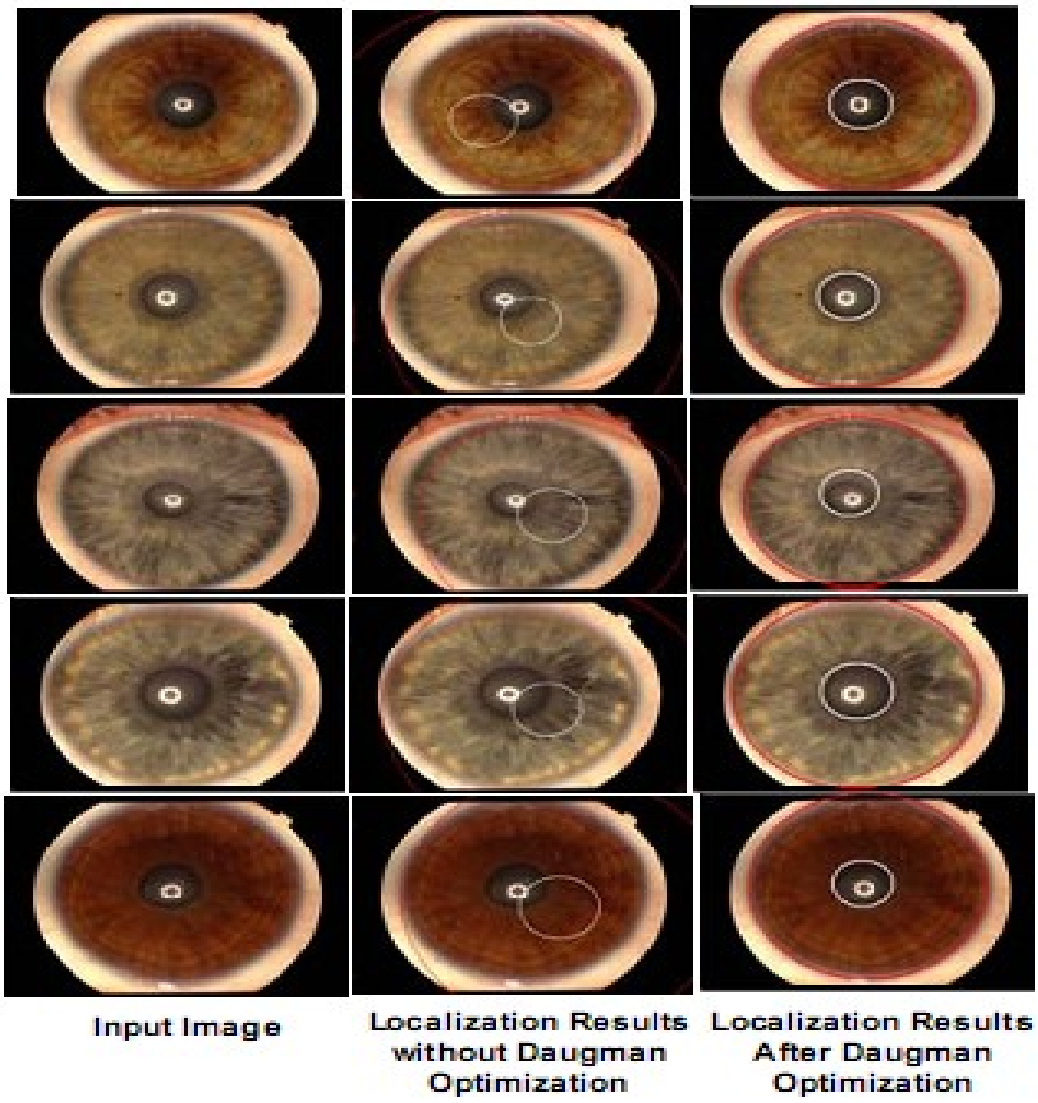


Figure Flowchart of optimized Daugman's localization algorithm operation.

Figure 1.6



Localization result
Figure 1.7

Data base	Number of samples	Daugman's Algorithm		Daugman's optimization	
		Fill	Success	Fill	Success
UPOL	384	75%	25%	0%	100%

The proposed algorithm is tested by applying it on UPOL database that includes about 384 images for 128 persons the localization successful percentage was 100%.

3.3 ADVANTAGES

The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

- It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.
- The iris is mostly flat and its geometric configuration is only controlled by two complementary muscles (the sphincter pupillae and dilator pupillae), which control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.
- The iris has a fine texture that – like fingerprints – is determined randomly during embryonic gestation. Even genetically identical individuals have completely independent iris textures, whereas DNA (genetic "fingerprinting") is not unique for the about 1.5% of the human population who have a genetically identical monozygotic twin.
- An iris scan is similar to taking a photograph and can be performed from about 10 cm to a few meters away. There is no need for the person to be identified to touch any equipment that has recently been touched by a stranger, thereby eliminating an objection that has been raised in some cultures against finger-print scanners, where a finger has to touch a surface, or retinal scanning, where the eye can be brought very close to a lens (like looking into a microscope lens).
- Some argue that a focused digital photograph with an iris diameter of about 200 pixels contains much more long-term stable information than a fingerprint.
- The originally commercially deployed iris recognition algorithm, John Daugman's IrisCode, has an unprecedented false match rate (better than 10^{-11}).
- While there are some medical and surgical procedures that can affect the colour and overall shape of the iris, the fine texture remains remarkably stable over many decades. Some iris identifications have succeeded over a period of about 30 years.

3.4 Disadvantages

- Iris scanning is a relatively new technology and is incompatible with the very substantial investment that the law enforcement and immigration authorities of some countries have already made into fingerprint recognition.
- Iris recognition is very difficult to perform at a distance larger than a few meters and if the person to be identified is not cooperating by holding the head still and looking into the camera.
- As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates.
- As with other identification infrastructure (national residents databases, ID cards, etc.), civil rights activists have voiced concerns that iris-recognition technology might help governments to track individuals beyond their will.

3.5 SECURITY CONSIDERATIONS

Like with most other biometric identification technology, a still not satisfactorily solved problem with iris recognition is the problem of "live tissue verification". The reliability of any biometric identification depends on ensuring that the signal acquired and compared has actually been recorded from a live body part of the person to be identified, and is not a manufactured template. Many commercially available iris recognition systems are easily fooled by presenting a high-quality photograph of a face instead of a real face, which makes such devices unsuitable for unsupervised applications, such as door access-control systems. The problem of live tissue verification is less of a concern in supervised applications (e.g., immigration control), where a human operator supervises the process of taking the picture.

Methods that have been suggested to provide some defence against the use of fake eyes and irises include:

- Changing ambient lighting during the identification (switching on a bright lamp), such that the papillary reflex can be verified and the iris image be recorded at several different pupil diameters
- Analysing the 2D spatial frequency spectrum of the iris image for the peaks caused by the printer dither patterns found on commercially available fake-iris contact lenses
- Analysing the temporal frequency spectrum of the image for the peaks caused by computer displays

- Using spectral analysis instead of merely monochromatic cameras to distinguish iris tissue from other material
- Observing the characteristic natural movement of an eyeball (measuring nystagmus, tracking eye while text is read, etc.)
- Testing for retinal retroreflection (red-eye effect)
- Testing for reflections from the eye's four optical surfaces (front and back of both cornea and lens) to verify their presence, position and shape
- Using 3D imaging (e.g., stereo cameras) to verify the position and shape of the iris relative to other eye features

A 2004 report by the German Federal Office for Information Security noted that none of the iris-recognition systems commercially available at the time implemented any live-tissue verification technology. Like any pattern-recognition technology, live-tissue verifiers will have their own false-reject probability and will therefore further reduce the overall probability that a legitimate user is accepted by the sensor.

4. CONCLUSION

Biometrics is a truly emerging market with great potential for success. Its roots may be in science fiction, but it is part of today's science and technology fact. In the near future, we will come to rely on biometric technology to protect our property, assets, and the people we love. We will see this technology become a secure and trusted form of authentication with uses varying from controlling access to personal information devices, to securing buildings and enabling eCommerce.

An important point to be noted in constructing a biometric system is that it should be based upon a distinguishable trait. For eg: Law enforcement has used finger prints to identify people. There is a great deal of scientific data supporting the idea that "no fingerprints are alike". All biometric systems capture data from individuals. Once these dates have been captured by the system, they can be forwarded to any location and put to many different uses which are capable of compromising on an individual's privacy. A good biometric system is one that is of low cost, fast, accurate, and easy to use.

5. REFERENCES

www.wikipedia.org

www.findbiometrics.com

www.biometrics.org

www.ti.com