www.final-yearprojects.co.cc | www.troubleshoot4free.com/fyp/

IRIS SCANNING

A SEMINAR REPORT

Submitted by

MARIYATH K.A

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE & ENGINEERING

SCHOOL OF ENGINEERING

COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY,

KOCHI-682 022

NOVEMER 2008

www.final-yearprojects.co.cc | www.troubleshoot4free.com/fyp/

DIVISION OF COMPUTER SCIENCE & ENGINEERING

SCHOOL OF ENGINEERING

COCHIN UNIVERSITY OF SCIENCE & TECHNOLOGY,

KOCHI-682022

Certificate

Certified that this is a bonafide record of the seminar work entitled

"IRIS SCANNING"

done by the following student

MARIYATH K.A

Of the VII th semester Computer Science and Engineering in the year 2008 in partial fulfillment of the requirements to the award of Degree of Bachelor of Technology in Computer Science and Engineering of Cochin University of Science and Technology

Mrs. Rahna P Muhammad
Seminar Guide

Dr. David Peter S
Head of the Department

Date:

ABSTRACT

Iris Scanning is a method of biometric authentication that uses pattern recognition technique based on high resolution of the irises of an individual eye. Biometrics is an automated method of capturing a person's unique biological data that distinguishes him or her from another individual. Iris recognition has emerged as one of the most powerful and accurate identification techniques in the modern world. It has proven to be most fool proof technique for the identification of individuals with out the use of cards. PIN's and passwords. It facilitates automatic identification where by electronic transactions or access to places, information or accounts are made easier, quicker and more secure.

www.final-yearprojects.co.cc | www.troubleshoot4free.com/fyp/

ACKNOWLEDGEMENT

At the outset, we thank the lord almighty for the grace, strength and hope to make our endeavor a success

We express our deep felt gratitude to **Dr. David Peter S**, Head of the Division, Computer science for his constant encouragement.

I profoundly grateful to **Mrs. Rahna P Muhammad** Lecturer ,Department of Computer Science , my mentor and seminar guide for her valuable Guidance support ,suggestions and encouragement

Further more I would like to thank all others especially our parents and numerous friends. This seminar would not have been a success without the inspiration, valuable suggestions and moral support from the through out its course

MARIYATH K.A

www.final-yearprojects.co.cc | www.troubleshoot4free.com/fyp/

TABLE OF CONTENTS

www.final-yearprojects.co.cc | www.troubleshoot4free.com/fyp/

LIST OF FIGURES

1. INTRODUCTION

In today's information age it is not difficult to collect data about an individual and use that information to exercise control over the individual. Individuals generally do not want others to have personal information about them unless they decide to reveal it. With the rapid development of technology, it is more difficult to maintain the levels of privacy citizens knew in the past. In this context, data security has become an inevitable feature. Conventional methods of identification based on possession of ID cards or exclusive knowledge like social security number or a password are not altogether reliable. ID cards can be almost lost, forged or misplaced: passwords can be forgotten. Such that an unauthorized user may be able to break into an account with little effort. So it is need to ensure denial of access to classified data by unauthorized persons. Biometric technology has now become a viable alternative to traditional identification systems because of its tremendous accuracy and speed. Biometric system automatically verifies or recognizes the identity of a living person based on physiological or behavioral characteristics. Since the persons to be identified should be physically present at the point of identification, biometric techniques gives high security for the sensitive information stored in mainframes or to avoid fraudulent use of ATMs.This paper explores the concept of Iris recognition which is one of the most popular biometric techniques. This technology finds applications in diverse fields.

1.1 Biometrics-future of identity

Biometric dates back to ancient Egyptians who measured people to identify them. Biometric devices have three primary components.

1. Automated mechanism that scans and captures a digital or analog image of a living personal characteristic
2. Compression, processing, storage and comparison of image with a stored data.
3. Interfaces with application systems.

A biometric system can be divided into two stages: the enrolment module and the identification module. The enrolment module is responsible for training the system to

identity a given person. During an enrolment stage, a biometric sensor scans the person's physiognomy to create a digital representation. A feature extractor processes the representation to generate a more compact and expressive representation called a template. For an iris image these include the various visible characteristics of the iris such as contraction, Furrows, pits, rings etc. The template for each user is stored in a biometric system database. The identification module is responsible for recognizing the person. During the identification stage, the biometric sensor captures the characteristics of the person to be identified and converts it into the same digital format as the template. The resulting template is fed to the feature matcher, which compares it against the stored template to determine whether the two templates match.

The identification can be in the form of verification, authenticating a claimed identity or recognition, determining the identity of a person from a database of known persons. In a verification system, when the captured characteristic and the stored template of the claimed identity are the same, the system concludes that the claimed identity is correct. In a recognition system, when the captured characteristic and one of the stored templates are the same, the system identifies the person with matching template.

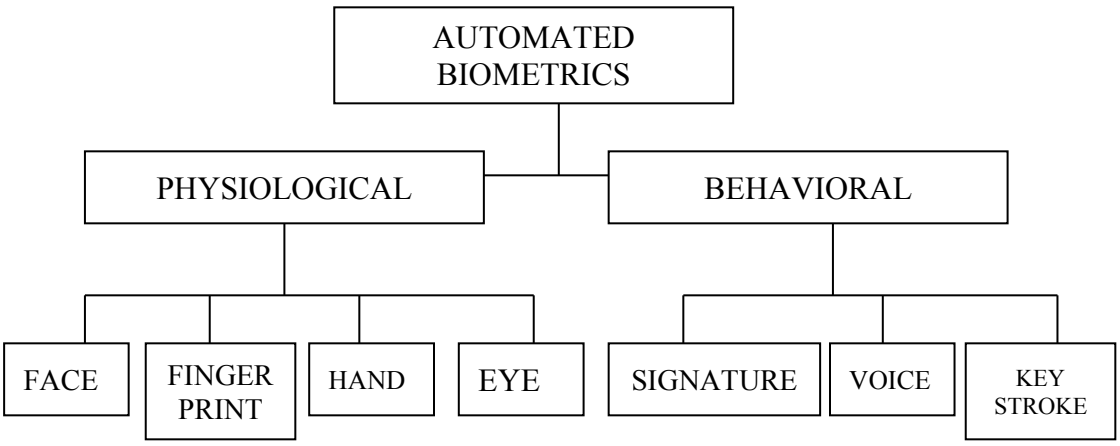

Fig 1.1 Topology of identification methods

Biometrics encompasses both physiological and behavioral characteristics. A physiological characteristic is a relatively stable physical feature such as finger print, iris pattern, retina pattern or a Facial feature. A behavioral trait in identification is a person's

signature, keyboard typing pattern or a speech pattern. The degree of interpersonal variation is smaller in a physical characteristic than in a behavioral one. For example, the person's iris pattern is same always but the signature is influenced by physiological characteristics.

Disadvantages

Even though conventional methods of identification are indeed inadequate, the biometric technology is not as pervasive and wide spread as many of us expect it to be. One of the primary reasons is performance. Issues affecting performance include accuracy, cost, integrity etc.

Accuracy

Even if a legitimate biometric characteristic is presented to a biometric system, correct authentication cannot be guaranteed. This could be because of sensor noise, limitations of processing methods, and the variability in both biometric characteristic as well as its presentation.

Cost

Cost is tied to accuracy; many applications like logging on to a pc are sensitive to additional cost of including biometric technology.

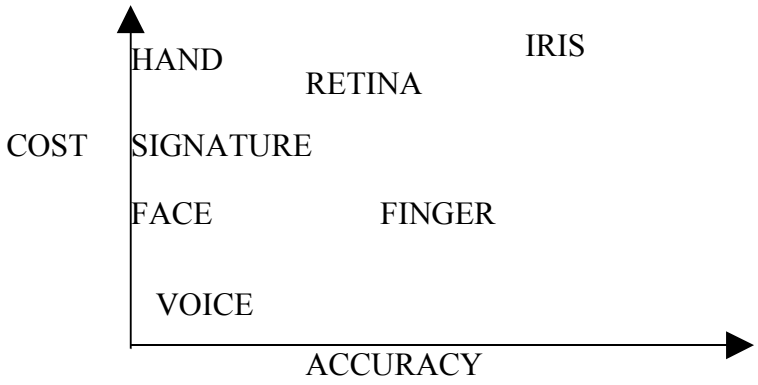

Fig 1.2. Comparison between cost and accuracy

2. IRIS RECOGNITION

Iris identification technology is a tremendously accurate biometric. Iris recognition leverages the unique features of the human iris to provide an unmatched identification technology. So accurate are the algorithms used in iris recognition that the entire planet could be enrolled in an iris database with only a small chance of false acceptance or false rejection. The technology addresses the FTE (Failure to Enroll) problems which lessen the effectiveness of other biometrics. Only the iris recognition technology can be used effectively and efficiently in large scale identification implementations. The tremendous accuracy of iris recognition allows it, in many ways, to stand apart from other biometric technologies.

2.1 Anatomy ,physiology and development of the iris

The word IRIS dates from classical times (a rainbow). The iris is a Protective internal organ of the eye. It is easily visible from yards away as a colored disk, behind the clear protective window of the cornea, surrounded by the white tissue of the eye. It is the only internal organ of the body normally visible externally. It is a thin diaphragm stretching across the anterior portion of the eye and supported by lens. This support gives it the shape of a truncated cone in three dimensions. At its base the eye is attached to the eye's ciliary body. At the opposite end it opens into a pupil. The cornea and the aqueous humor in front of the iris protect it from scratches and dirt, the iris is installed in its own casing. It is a multi layered structure. It has a pigmented layer, which forms a coloring that surrounds the pupil of the eye. One feature of this pupil is that it dilates or contracts in accordance with variation in light intensity.

The human iris begins to form during the third month of gestation. The structures creating its distinctive pattern are completed by the eighth month of gestation hut pigmentation continues in the first years after birth. The layers of the iris have both ectodermic and embryological origin, consisting of: a darkly pigmented epithelium, pupillary dilator and sphincter muscles, heavily vascularized stroma and an anterior layer chromataphores with a genetically determined density of melanin pigment granules. The combined effect is a visible pattern displaying various distinct features such as arching

ligaments, crypts, ridges and zigzag collaratte. Iris color is determined mainly by the density of the stroma and its melanin content, with blue irises resulting from an absence of pigment: long wavelengths are penetrates and is absorbed by the pigment epithelium, while shorter wavelengths are reflected and scattered by the stroma. The heritability and ethnographic diversity of iris color have long been studied. But until the present research, little attention had been paid to the achromatic pattern complexity and textural variability of the iris among individuals.

A permanent visible characteristic of an iris is the trabecular mesh work, a tissue which gives the appearance of dividing the iris in a radial fashion. Other visible characteristics include the collagenous tissue of the stroma, ciliary processes, contraction furrows, crypts, rings, a corona and pupillary frill coloration and sometimes freckle. The striated anterior layer covering the trabecular mesh work creates the predominant texture with visible light.

Fig 2.1. A Typical Iris

2.2 Iris as a powerful identifier

Iris is the focus of a relatively new means of biometric identification. The iris is called the living password because of its unique, random features. It is always with you and can not be stolen or faked. The iris of each eye is absolutely unique. The probability that any two irises could be alike is one in 10 to 78^{th} power — the entire human population of the earth is roughly 5.8 billion. So no two irises are alike in their details, even among identical twins. Even the left and right irises of a single person seem to be highly distinct. Every iris has a highly detailed and unique texture that remains stable over decades of life. Because of the texture, physiological nature and random generation of an iris artificial duplication is virtually impossible.

The properties of the iris that enhance its suitability for use in high confidence identification system are those following.

1. Extremely data rich physical structure about 400 identifying features
2. Genetic independence no two eyes are the same.
3. Stability over time.
4. Its inherent isolation and protection from the external environment.
5. The impossibility of surgically modifying it without unacceptable risk to vision.
6. Its physiological response to light, which provides one of several natural tests against artifice.
7. The ease of registering its image at some distance forms a subject without physical contact. unobtrusively and perhaps inconspicuously
8. It intrinsic polar geometry which imparts a natural co-ordinate system and an origin of co-ordinates
9. The high levels of randomness in it pattern inter subject variability spanning 244 degrees of freedom - and an entropy of 32 bits square million of iris tissue.

2.3 History and development

The idea of using patterns for personal identification was originally proposed in 1936 by ophthalmologist Frank Burch. By the 1980's the idea had appeared in James Bond films, but it still remained science fiction and conjecture. In 1987, two other ophthalmologists Aram Safir and Leonard Flom patented this idea and in 1987 they asked John Daugman to try to create actual algorithms for this iris recognition. These algorithms which Daugman patented in 1994 are the basis for all current iris recognition systems and products.

Daugman algorithms are owned by Iridian technologies and the process is licensed to several other Companies who serve as System integrators and developers of special platforms exploiting iris recognition in recent years several products have been developed for acquiring its images over a range of distances and in a variety of applications. One active imaging system developed in 1996 by licensee Sensar deployed special cameras in bank ATM to capture IRIS images at a distance of up to 1 meter. This active imaging system was installed in cash machines both by NCR Corps and by Diebold Corp in successful public trials in several countries during I997 to 1999. a new and smaller imaging device is the low cost "Panasonic Authenticam" digital camera for handheld, desktop, e-commerce and other information security applications. Ticket less air travel, check-in and security procedures based on iris recognition kiosks in airports have been developed by eye ticket. Companies in several, countries are now using Daughman's algorithms in a variety of products.

2.4 Science behind the technology

The design and implementation of a system for automated iris recognition can be subdivided in to 3.

1. image acquisition
2. iris localization and
3. Pattern matching

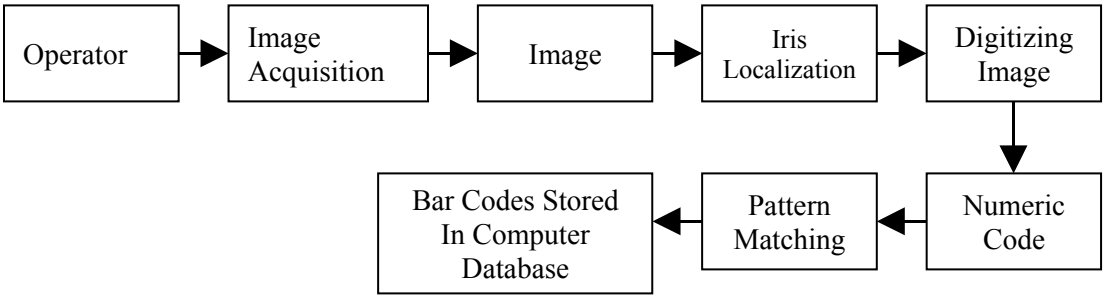

Fig 2.2 Block Diagram of Iris Recognition

2.4.1 Image acquisition

The iris recognition process begins with video-based image acquisition a process which deals with the capturing of a high quality image of the iris while remaining non-invasive to the human operator. There are 3 important requisites for this process

a) It is desirable to acquire images of the iris with sufficient resolution and sharpness to support recognition
b) It is important to have good contrast in the interior iris pattern without restoring to a level of illumination that annoys the Operator, that is adequate intensity of source constrained by operators comfort with brightness.
c) These images must be well framed without unduly constraining the operator. The widely used recognition system is the daugmen system which captures images with the iris diameter typically between 100 and 200 pixels from a distance of 15, 46 cm using a 330 mm lens.

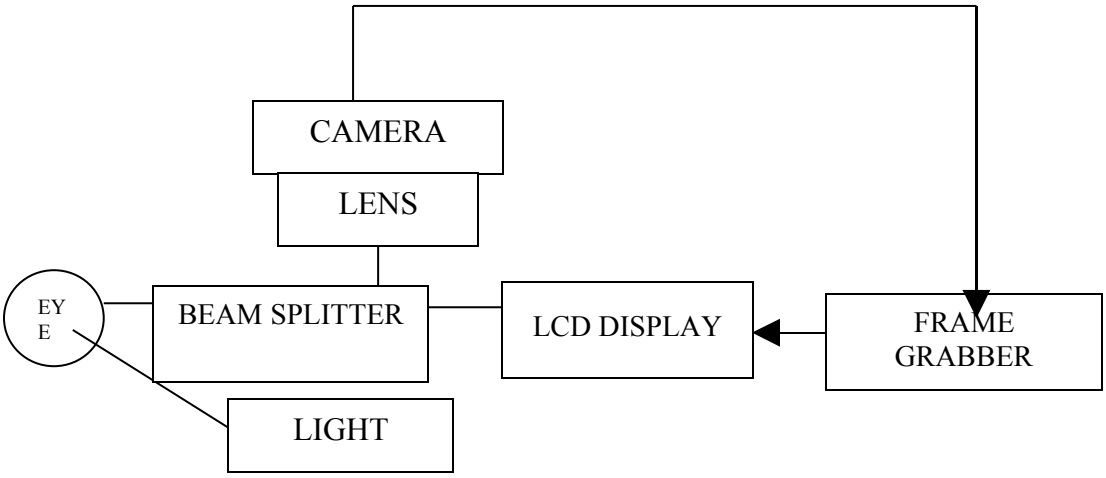

Fig 2.3 Image acquisition rings for automated iris recognition

Image acquisition is performed as follows. It uses LED based point light sources in conjunction with a wide angle camera no more than 3 feet from the subject's eye. By carefully positioning the light source below the operator, reflection of point source can be avoided in the imaged iris. The system makes use of light, which is visible to human eye. Infrared illumination can also be employed. This System requires the operator to self position his eye in front of the camera. It provides the operator with a live video feed back via beam splitter. This allows the operator to see what the camera is capturing and to adjust his position. Once a series of images of sufficient quality is acquired, it is automatically forwarded for subsequent processing.

2.4.2 Iris localization

Image acquisition of iris can be expected to yield an image containing only the iris. Rather image acquisition will capture the iris as part of a larger image that also contains data derived from the surrounding eye region. Prior to performing iris pattern

matching it is important to localize that portion of the image that corresponds to iris. Iris localization is a process that delimits the iris from the rest of the acquired image. After the camera situates the eye, the Daugman's algorithm narrows in from the right and left of the iris to locate its outer edge. This horizontal approach accounts for obstruction caused by the eyelids. It simultaneously locates the inner edge of the iris, excluding the lower 90^0 because of inherent moisture and lighting issues.

Conversion of an iris image into a numeric code that can be easily manipulated is essential to its use. This process developed by John Daugman. Permits efficient comparison of irises. Upon the location of the iris, an iris code is computed based on the information from a set of Gabor wavelets. The Gabor wavelet is a powerful tool to make iris recognition practical. These wavelets are specialized filter banks that extract information from a signal at a variety of locations and scales. The filters are members of a family of functions developed by Dennis Gabor, that optimizes the resolution in both spatial and frequency domains. The 2-D Gabor wavelets filter and map segments of iris into hundreds of vectors. The wavelets of various sizes assign values drawn from the orientation and spatial frequency of select areas, bluntly referred to as the "what" of the sub-image, along with the position of these areas, bluntly referred to as the "where". The "what" and where are used to form the Iris Code. Not all of iris is used: a portion of the top, as well as 45^0 of the bottom is unused to account for eyelids and camera—light reflections. The iris Code is calculated using 8 circular bands that have been adjusted to the iris and pupil boundaries.

Iris recognition technology converts the visible characteristics of the iris into a 512 byte Iris Code, a template stored for future verification attempts. 5l2 bytes is a fairly compact size for a biometric template, but the quantity of information derived from the iris is massive. From the iris 11 mm diameters, Dr. Daugman's algorithms provide 3.4 bits of data per square mm. This density of information is such that each iris can be said to have 266 unique "spots", as opposed to 13- 60 for traditional biometric technology. This 266 measurement is cited in all iris recognition literature, after allowing for the algorithms for relative functions and for characteristics inherent to most human eyes. Dr.

Daugman concludes that 173 “independent binary degrees of freedom can be extracted from his algorithm-and exceptionally large number fur a biometric, for future identification, the database will not be comparing images of iris, but rather hexadecimal representations of data returned by wavelet filtering and mapping. The Iris Code for an iris is generated within one second. Iris Code record is immediately encrypted and cannot be reverse engineered.

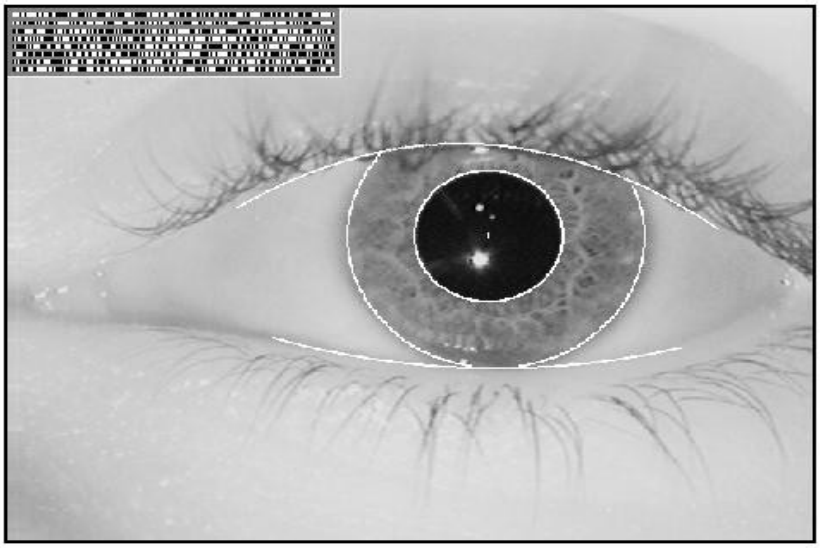

Fig 2.4 Iris code

2.4.3 Pattern matching

When a live iris is presented for comparison, the iris pattern is processed and encoded into 512 byte Iris Code. The Iris Code derived from this process is compared

with previously generated Iris Code. This process is called pattern matching. Pattern matching evaluates the goodness of match between the newly acquired iris pattern and the candidate's data base entry. Based on this goodness of match final decision is taken whether acquired data does or doesn't come from the same iris as does the database entry.

Pattern matching is performed as follows. Using integer XOR logic in a single clock cycle, a long vector of each to iris code can be XORed to generate a new integer. Each of whose bits represent mismatch between the vectors being compared. The total number of 1s represents the total number of mismatches between the two binary codes. The difference between the two recodes is expressed as a fraction of mismatched bits termed as hamming distance. For two identical Iris Codes, the hamming distance is Zero. For perfectly unmatched Iris Codes, the hamming distance is 1. Thus iris patterns are compared. The entire process i.e. recognition process takes about 2 seconds. A key differentiator for iris recognition is its ability to perform identification using a one to many search of a database, with no limitation on the number of iris code records contained there in.

2.5 Mathematical explanation

An “Iris Code” is constructed by demodulation of the iris pattern. This process uses complex-valued 2D Gabor wavelets to extract the structure of the iris as a sequence of phasors, whose phase angles are quantized to set the bits in the first code.

This process is performed in a doubly—dimensionless polar co-ordinate system that is invariant to the size of the iris, and also invariant to the dilation diameter of the pupil within the iris.

The demodulating wavelets are parameterized with four degrees-of-freedom: Size, orientation and two positional co-ordinates. They span several octaves in size, in order to extract iris structure at many different scales of analysis. Because the information extracted from the iris is inherently described in terms of phase, it is insensitive to contrast, camera gain and illumination level. The phase description is very compact, requiring only 256 bytes to represent each iris pattern. These 2D wavelets are optimal encoders under the inherent Heisenberg—Weyl uncertainty relation for extraction of information in conjoint spatial-spectral representations.

The recognition of irises by their recodes is based upon the failure of a test of statistical independence. Any given Iris Code is statistically guaranteed to pass a test of independence against any Iris Code computed from a different eye; but it will uniquely fail the same test against the eye from which it was composed. Thus the key to iris recognition is the failure of’ a test of statistical independence.

2.5.1 Accuracy

The Iris Code constructed from these Complex measurements provides such a tremendous wealth of data that iris recognition offers level of accuracy orders of magnitude higher than biometrics. Some statistical representations of the accuracy follow:

- The odds of two different irises returning a 75% match (i.e. having Hamming Distance of 0.25): 1 in 10^{16}.
- Equal Error Rate (the point at which the likelihood of a false accept and false reject are the same): 1 in 12 million.
- The odds of two different irises returning identical Iris Codes: 1 in 10^{52}

Other numerical derivations demonstrate the unique robustness of these algorithms. A person's right and left eyes have a statistically insignificant increase in similarity: 0.0048 on a 0.5 mean. This serves to demonstrate the hypothesis that iris shape and characteristic are phenotype - not entirely; determined by genetic structure. The algorithm can also account for the iris: even if 2/3 of the iris were completely obscured, accurate measure of the remaining third would result in an equal error rate of 1 in 100000.

Iris recognition can also accounts for those ongoing changes to the eye and iris which are defining aspects of living tissue. The pupil's expansion and contraction, a constant process separate from its response to light, skews and stretches the iris. The algorithms account for such alteration after having located at the boundaries of the iris. Dr. Daugman draws the analogy to a 'homogenous rubber sheet" which, despite its distortion retains certain consistent qualities. Regardless of the size of the iris at any given time, the algorithm draws on the same amount or data, and its resultant Iris Code is stored as a 512 byte template. A question asked of all biometrics is there is then ability to determine fraudulent samples. Iris recognition can account for this in several ways the detection of pupillary changes, reflections from the cornea detection of contact lenses atop the cornea and use of infrared illumination to determine the state of the sample eye tissue.

2.5.2 Decision Environment

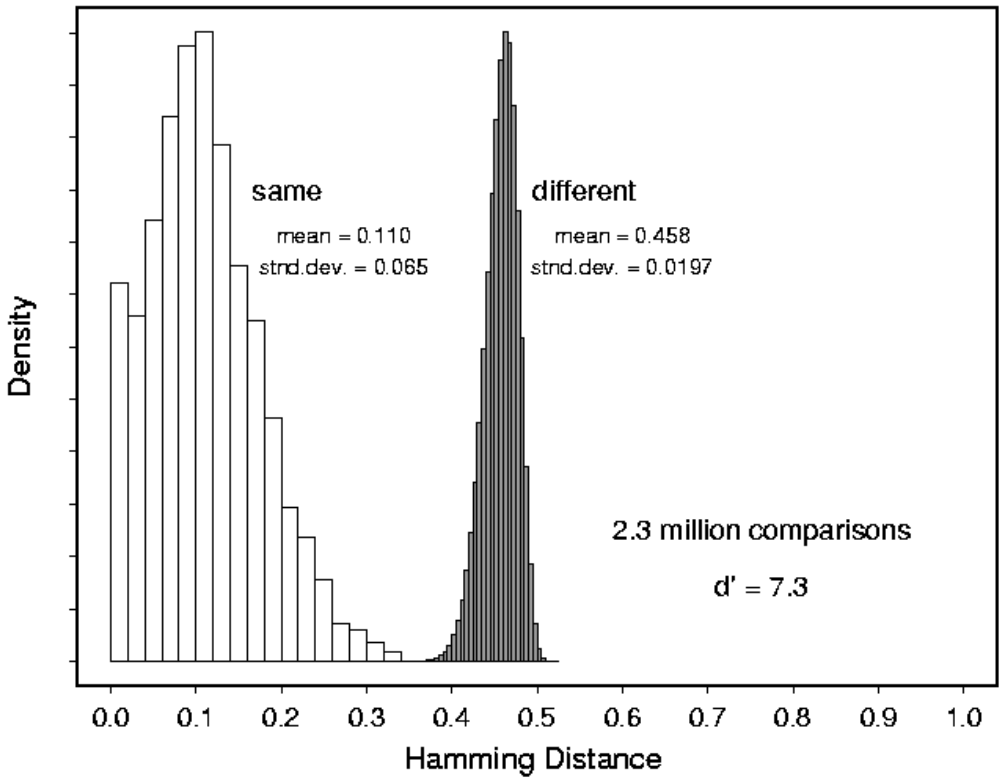

Fig 2.5 Decision environment

The performance of any biometric identification scheme is characterized by its "Decision Environment'. This is a graph superimposing the two fundamental histograms of similarity that the test generates: one when comparing biometric measurements from the SAME person (different times, environments, or conditions), and the other when comparing measurements from DIFFERENT persons. When the biometric template of a presenting person is compared to a previously enrolled database of templates to

determine the Persons identity, a criterion threshold (which may be adaptive) is applied to each similarly score. Because this determines whether any two templates are deemed to be “same” or “different”, the two fundamental distributions should ideally be well separated as any overlap between them causes decision errors.

One metric for “decidability”, or decision—making power, is d. This is defined as the separation between the means of two distributions, divided by the square root of their average variance. One advantage of using d’ for comparing, the decision-making power of biometrics is the fact that it does not depend on any choice about the decision threshold used. Which of course may vary from liberal to conservative when selecting the trade-off between the False Accept Rate (FAR) and False Reject Rate (FRR)? The d’ metric is a measure of the inherent degree to which any decrease in one error rate must be paid for by an increase in the other error rate, when decision thresholds are varied. It reflects the intrinsic separability of the two distributions.

Decidability metrics such as d’ can he applied regardless of what measure of similarity a biometric uses. In the particular case of iris recognition, the similarly measure is a Hamming distance: the fraction of bits in two iris Codes that disagree. The distribution on the left in the graph shows the result when different images of the same eye are compared: typically about 10% of the bits may differ. But when Iris Codes from different eyes are compared: With rations to look for and retain the best match. The distribution on the right is the result. The fraction of disagreeing bits is very tightly packed around 45%. Because of the narrowness of this right-hand distribution, which belongs to the family of binomial extreme-value distributions, it is possible to make identification decisions with astronomical levels of confidence. For example, the odds of two different irises agreeing just by chance in more than 75 of their Iris Code bits, is only one in 10-to-the- 14^{th} power. These extremely low probabilities of getting a False Match enable the iris recognition algorithms to search through extremely large databases, even of a national or planetary scale, without confusing one Iris Code for another despite so many error opportunities.

2.6 Comparison between genetically identical iris patterns

Although the striking visual similarity of identical twins reveals the genetic penetrance of overall facial appearance, a comparison of genetically identical irises reveals just the opposite for iris patterns: the iris texture is an epigenetic phenotypic feature, not a genotypic feature. A convenient source of genetically identical irises is the right and left pair from any given person. Such pairs have the same genetic relationship as the four irises of two identical twins, or indeed in the probable future, the 2N irises of N human clones. Eye color of course has high genetic penetrance, as does the overall statistical quality of the iris texture, but the textural details are uncorrelated and independent even in genetically identical pairs. So performance is not limited by the birth rate of identical twins or the existence of genetic relationships.

2.7 Uniqueness of iris code

2.7.1 Independence of bits across iris codes

It is important to establish and to measure the amount of independent variation both within an iris and between different irises. There are correlations within an iris because local structure is self-predicting; for example, furrows tend to propagate themselves radially. Such self-correlations limit the number of degrees of freedom within irises. But even more important is the question of whether systematic correlations exist between different irises.

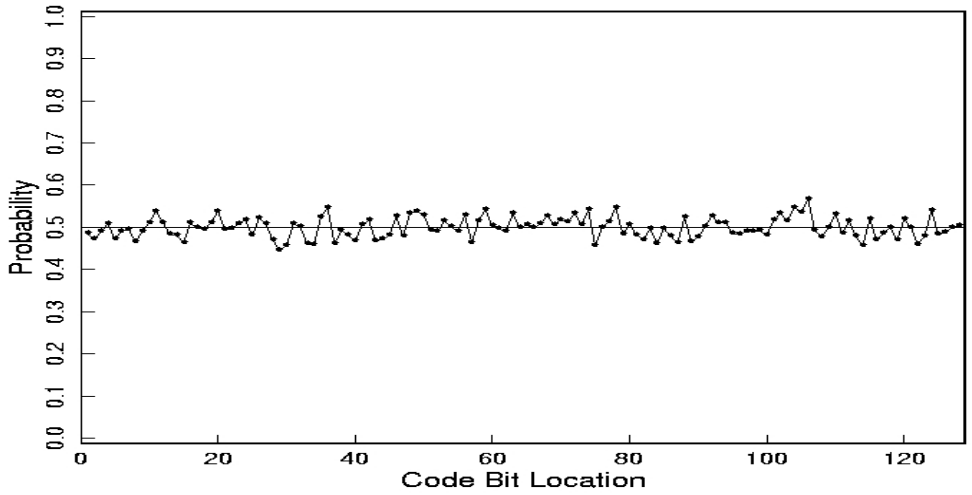

Fig 2.6. Independence of bits across iris codes

This probability distribution suggests that they do not. It plots the probability that bits in different positions within the Iris Code are set to 1, for a randomly sampled population of different Iris Codes. The fact that this distribution hovers near 0.5 indicates that all Iris Code bits are equally likely to be 0 or 1. This property makes Iris Codes "maximum entropy" codes in a bit-wise sense. The fact that this distribution is uniform indicates that different irises do not systematically share any common structure. For example, if most irises had a furrow or crypt in the 12-o'clock position, then the plot shown here would not be flat. The recognition of persons by their Iris Codes is based Upon the failure of a test of statistical independence. The plot shown here illustrates why any given Iris Code is "statistically guaranteed" to pass a test of independence against any Iris Code computed from a different eye.

2.8 Binomial distribution of iris code hamming

2.8.1 **Distances**

The Histogram given below shows the outcomes of 2,307,025 comparisons between different pairs of irises. For each pair comparison, the percentage of their Iris Code bits that disagreed was computed and tallied as a fraction. Because of the zero-mean property of the wavelet demodulators, the computed coding bits are equally likely

to be 1 or 0. Thus when any corresponding bits of two different Iris Codes are compared, each of the four combinations (00), (01), (10), (11) has equal probability. In two of these cases the bits agree, and in the other two they disagree. Therefore one would expect on average 50% of the bits between two different Iris Codes to agree by chance. The above histogram presenting comparisons between 2.3 million different pairings of irises shows a mean fraction of 0.499 of their Iris Code bits agreeing by chance.

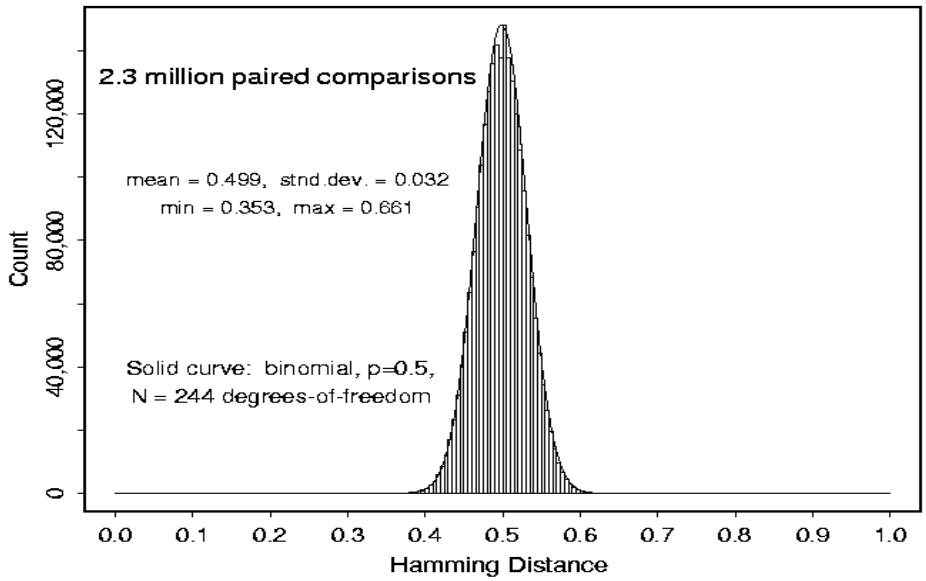

Fig 2.7 .B inomial distribution of iris code hamming distances

The standard deviation of this distribution, 0.032, reveals the effective number of independent bits (binary degrees of freedom) when Iris Codes are compared. Because of correlations within irises and within computed Iris Codes, the number of degrees of freedom is considerably smaller than the number of bits computed. But even correlated Bernoulli trials (coin tosses) generate binomial distributions; the effect of their

correlations is equivalent to reducing the effective number of Bernoulli trials. For comparisons between different pairs of Iris Codes, the distribution shown above corresponds to that for the fraction of "heads" that one would get in runs of 244 tosses of a fair coin. This is a binomial distribution, with parameters p=q=0.5 and N=244 Bernoulli trials (coin tosses). The solid curve in the above histogram is a plot of such a binomial probability distribution. It gives an extremely exact fit to the observed distribution, as may be seen by comparing the solid curve to the data histogram.

The above two aspects show that Hamming Distance comparisons between different Iris Codes are binomially distributed, with 244 degrees of freedom. The important corollary of this conclusion is that the tails of such distributions are dominated by factorial combinatorial factors, which attenuate at astronomic rates. This property makes it extremely improbable that two different Iris Codes might happen to agree just by chance in, say, more than 2/3rds of their bits (making a Hamming Distance below 0.33 in the above plot). The confidence levels against such an occurrence are the reason why iris recognition can afford to search extremely large databases, even on a national scale, with negligible probability of making even a single false match.

2.9 Commensurability of iris codes

A critical feature of this coding approach is the achievement of commensurability among iris codes, by mapping all irises into a representation having universal format and constant length, regardless of the apparent amount of iris detail. In the absence of commensurability among the codes, one would be faced with the inevitable problem of comparing long codes with short codes, showing partial agreement and partial disagreement in their lists of features. It is not obvious mathematically how one would make objective decisions and compute confidence levels on a rigorous basis in such a situation. This difficulty has hampered efforts to automate reliably the recognition of fingerprints. Commensurability facilitates and objectifies the code comparison process, as well as the computation of confidence.

2.10 Advantages

- Highly protected, internal organ of the eye
- Externally visible; patterns imaged from a distance
- Iris patterns possess a high degree of randomness
    - Variability: 244 degrees-of-freedom
    - Entropy: 3.2 bits per square-millimeter
    - Uniqueness: set by combinatorial complexity
- Changing pupil size confirms natural physiology
- Pre-natal morphogenesis (7th month of gestation)
- Limited genetic penetrance of iris patterns
- Patterns apparently stable throughout life
- Encoding and decision-making are tractable
- Image analysis and encoding time: 1 second
- Decidability index (d-prime): d' = 7.3 to 11.4
- Search speed: 100,000 Iris Codes per second

2.11 Disadvantages of using iris for identification

- Small target (1 cm) to acquire from a distance (1m)
- Located behind a curved, wet, reflecting surface
- Obscured by eyelashes, lenses, reflections
- Partially occluded by eyelids, often drooping
- Deforms non-elastically as pupil changes size
- Illumination should not be visible or bright
- Some negative connotations

2.12 Applications

Iris-based identification and verification technology has gained acceptance in a number of different areas. Application of iris recognition technology can he limited only by imagination. The important applications are those following:

- **ATM's and iris recognition:** in U.S many banks incorporated iris recognition technology into ATM's for the purpose of controlling access to one's bank accounts. After enrolling once (a "30 second" process), the customer need only approach the ATM, follow the instruction to look at the camera, and be recognized within 2-4 seconds. The benefits of such a system are that the customer who chooses to use bank's ATM with iris recognition will have a quicker, more secure transaction.

- **Tracking Prisoner Movement:** The exceptionally high levels of accuracy provided by iris recognition technology broadens its applicability in high risk, high-security installations. Iris scan has implemented their devices with great success in prisons in Pennsylvania and Florida. By this any prison transfer or release is authorized through biometric identification. Such devices greatly ease logistical and staffing problems.

Applications of this type are well suited to iris recognition technology. First, being fairly large, iris recognition physical security devices are easily integrated into the mountable, sturdy apparatuses needed or access control, The technology's phenomenal accuracy can be relied upon to prevent unauthorized release or transfer and to identify repeat offenders re-entering prison under a different identity.

- Computer login: The iris as a living password.
- National Border Controls: The iris as a living password.
- Telephone call charging without cash, cards or PIN numbers.
- Ticket less air travel.
- Premises access control (home, office, laboratory etc.).
- Driving licenses and other personal certificates.
- Entitlements and benefits authentication.
- Forensics, birth certificates, tracking missing or wanted person
- Credit-card authentication.
- Automobile ignition and unlocking; anti-theft devices.
- Anti-terrorism (e.g.:— suspect Screening at airports)
- Secure financial transaction (e-commerce, banking).
- Internet security, control of access to privileged information.
- “Biometric—key Cryptography “for encrypting/decrypting messages.

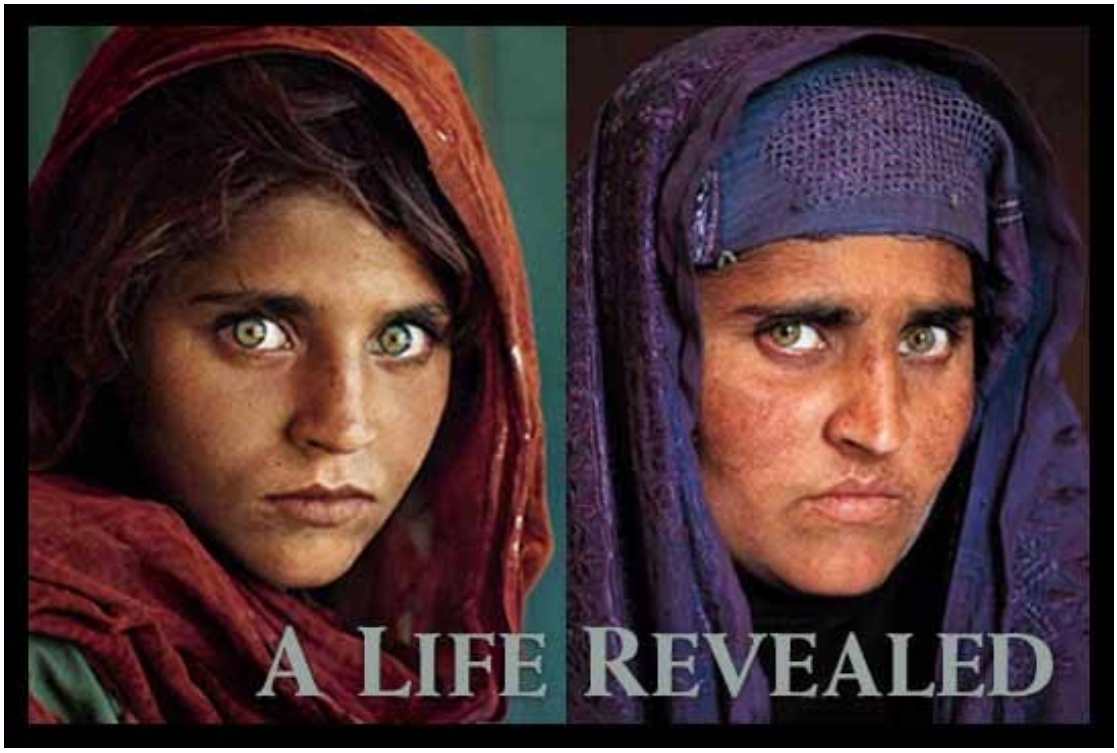

Fig 2.8 .Identifying the mystery woman

Iris recognition system is also finding unexpected applications. The best know example involved using iris recognition to confirm the identification of a mysterious young afghan woman named Sharbat Gula originally photographed by Steve McCurry in 1984.Some 18 years later, McCurry photographed Sharbat Gula in Afghanistan .At the behest of National Geographic, Dr.John Dougman,developer of the Iris recognition system, then compared the irises in the photographs using his algorithms. He concluded that the eyes were a match.

2.13 Iris Recognition: Issues

Every biometric technology has its own challenges. When reviewing test results, it is essential to consider the environment and protocols of the test. Much industry testing is performed in laboratory settings on images acquired in ideal conditions. Performance in a real world application may result in very different performance as there is a learning curve for would-be user of the system and not every candidate will enroll properly or quickly the first time. There are some issues which affect the functionality and applicability of iris recognition technology in particular.

The technology requires a certain amount of user interaction the enroller must hold still in a certain spot, even if only momentarily. It would be very difficult to enroll or identify a non-cooperative subject. The eye has to have a certain degree of lighting to allow the camera to capture the iris; any unusual lighting situation may affect the ability of the camera to acquire its subject. Lastly, as with any biometric, a backup plan must be in place if the unit becomes inoperable. Network crashes, power failure, hardware and software problems are but a few of the possible ways in which a biometric system would become unusable. Since iris technology is designed to be an identification technology, the fallback procedures may not be as fully developed as in a recognition schematic. Though these issues do not reduce the exceptional effectiveness of iris recognition technology, they must be kept in mind, should a company decide to implement on iris-based solution.

www.final-yearprojects.co.cc | www.troubleshoot4free.com/fyp/

3 CONCLUSION

The technical performance capability of the iris recognition process far surpasses that of any biometric technology now available. Iridian process is defined for rapid exhaustive search for very large databases: distinctive capability required for authentication today. The extremely low probabilities of getting a false match enable the iris recognition algorithms to search through extremely large databases, even of a national or planetary scale. As iris technology grows less expensive, it could very likely unseat a large portion of the biometric industry, e-commerce included; its technological superiority has already allowed it to make significant inroads into identification and security venues which had been dominated by other biometrics. Iris-based biometric technology has always been an exceptionally accurate one, and it may soon grow much more prominent.

4. REFERENCES

1. Daugman J (1999) "Wavelet demodulation codes, statistical independence, and pattern recognition." Institute of Mathematics and its Applications, Proc.2nd IMA-IP. London: Albion, pp 244 - 260.
2. Daugman J (1999) "Biometric decision landscapes." Technical Report No TR482, University of Cambridge Computer Laboratory.
3. Daugman J and Downing C J (1995) "Demodulation, predictive coding, and spatial vision." Journal of the Optical Society of America A, vol. 12, no. 4, pp 641 - 660.
4. 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, pp 1148 - 1160.
5. Daugman J (1985) "Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters." Journal of the Optical Society of America A, vol. 2, no. 7, pp 1160 - 1169.

WEB SITE

- http://www.cl.cam.ac.uk/~jgd1000/
- http://en.wikipedia.org/wiki/Iris_recognition