IRIS RECOGNITION-A BIOMETRIC TECHNOLOGY

submitted by:
Seema Sheoran
2008UIT146
6th sem
Information Technology
Malaviya National Institute of Technology, Jaipur

19th march, 2011
Abstract

Iris recognition is the process of recognizing a person by analysing the random pattern of the iris, which is unique for each person. This automated method is relatively young, existing in patent only since 1994.

The iris contains complex patterns of ligaments, furrows, ridges, crypts, rings and corona that allow algorithms to be produced that can be used to identify an individual. An IrisCode is created by encoding the variable structures of the iris. Daugmans iris recognition process for verification and identification involves comparing IrisCodes by performing Boolean XOR operations and computing a function called the Hamming Distance, as a measure of dissimilarity between any two irises.

Iris recognition systems are being used today to control physical access, to facilitate identity verification and for computer authentication. Real-world iris recognition applications have been implemented for airport and prison security, automatic teller machines, authentication using single sign-on, to replace ID cards, and to secure schools and hospitals. Based on the applications, reliability, ease of use, and software and hardware devices that currently support it, iris recognition technology has potential for widespread use.
8.4.2 Authentication Server

9 CONCLUSION
# List of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1</td>
<td>Physiology of eye</td>
<td>9</td>
</tr>
<tr>
<td>4.1</td>
<td>An IriScan model 2100 iris scanner</td>
<td>10</td>
</tr>
<tr>
<td>4.2</td>
<td>Circular iris location</td>
<td>11</td>
</tr>
<tr>
<td>4.3</td>
<td>Optimizing the image</td>
<td>11</td>
</tr>
<tr>
<td>5.1</td>
<td>Binomial distribution for 9.1 million cross-comparisons of independent iris templates. Hamming distances center at 0.5. [John Daugman, Cambridge University 2002]</td>
<td>15</td>
</tr>
<tr>
<td>5.2</td>
<td>Distribution of Hamming distances for template comparisons. The left peak is composed of comparisons of matching pairs of templates. [John Daugman, Cambridge University 2002]</td>
<td>16</td>
</tr>
<tr>
<td>8.1</td>
<td>Panasonics Authenticam&lt;sup&gt;TM&lt;/sup&gt; Enabled with Private Id&lt;sup&gt;TM&lt;/sup&gt; Software.</td>
<td>27</td>
</tr>
</tbody>
</table>
Chapter 1

INTRODUCTION

In today's information technology world, security for systems is becoming more and more important. The number of systems that have been compromised is ever increasing and authentication plays a major role as a first line of defence against intruders. The three main types of authentication are something you know (such as a password), something you have (such as a card or token), and something you are (biometric). Passwords are notorious for being weak and easily crackable due to human nature and our tendency to make passwords easy to remember or writing them down somewhere easily accessible. Cards and tokens can be presented by anyone and although the token or card is recognisable, there is no way of knowing if the person presenting the card is the actual owner. Biometrics, on the other hand, provides a secure method of authentication and identification, as they are difficult to replicate and steal. If biometrics is used in conjunction with something you know, then this achieves what is known as two-factor authentication. Two-factor authentication is much stronger as it requires both components before a user is able to access anything.

Iris recognition, a biometric, provides one of the most secure methods of authentication and identification thanks to the unique characteristics of the iris. Once the image of the iris has been captured using a standard camera, the authentication process, involving comparing the current subject’s iris with the stored version, is one of the most accurate with very low false acceptance and rejection rates. This makes the technology very useful in areas such as information security, physical access security, ATMs and airport security.

The technology is accurate, easy to use, non-intrusive, difficult to forge and, despite what people may think, is actually quite a fast system once initial enrolment has taken place. However, it does require the co-operation of the subject, needs specific hardware and software to operate and administrators need to ensure they have a fall back plan should the resources required to operate the system fail, for example power. Iris recognition technology does provide a good method of authentication to replace the current methods of passwords, token cards or PINs and if used in conjunction with something the user knows in a two-factor authentication system then the authentication becomes even stronger.
Chapter 2

BIOMETRIC TECHNOLOGY

Biometric technology is a technology that uses the measurements of a unique human attribute or feature in order to distinguish that person from all others. Characteristics fall into two categories:

- **Physiological** are related to the shape of the body. Examples are facial recognition - 2D, 3D, Thermographic; Retinal scanning; Iris scanning; Finger Scanning - fingertip, thumb, length, pattern; Palm Scanning - print, topography; Hand Geometry; Wrist/Hand Vein; Ear Shape etc.

- **Behavioural** are related to the behavior of a person. Examples are Voice Prints; Dynamic Signature Verification; Keystroke Dynamics etc.

Behavioural biometric systems tend to be less expensive than physical biometric systems but also less robust. Behavioural characteristics can be drawn from the dynamic attributes of the user, however these features may not necessarily be unique to one individual.

2.1 Modes of operation of a biometric system

A biometric system can operate in the following two modes:

1. **Verification**: A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. Can be done in conjunction with a smart card, username or ID number.

2. **Identification**: A one to many comparison of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.
2.2 Performance

The following are used as performance metrics for biometric systems:

1. **false accept rate or false match rate (FAR or FMR)** the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

2. **false reject rate or false non-match rate (FRR or FNMR)** the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

3. **receiver operating characteristic or relative operating characteristic (ROC)** The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR. A common variation is the Detection error trade-off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances (rarer errors).

4. **equal error rate or crossover error rate (EER or CER)** the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate.

5. **failure to enroll rate (FTE or FER)** the rate at which attempts to create a template from an input is unsuccessful. This is most commonly caused by low quality inputs.

6. **failure to capture rate (FTC)** Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly.

7. **template capacity** the maximum number of sets of data which can be stored in the system.
Chapter 3

IRIS RECOGNITION

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The automated method of iris recognition is relatively young, existing in patent only since 1994. Iris recognition is a physical biometric system.

3.1 Iris recognition- History

- In 1936, ophthalmologist Frank Burch proposed the concept of using iris patterns as a method to recognize an individual.
- In 1985, Drs. Leonard Flom and Aran Safir, ophthalmologists, proposed the concept that no two irides are alike, and were awarded a patent for the iris identification concept in 1987. Dr. Flom approached Harvard Professor Dr. John Daugman to develop an algorithm to automate identification of the human iris.
- In 1993, the Defense Nuclear Agency began work to test and deliver a prototype unit, which was successfully completed by 1995 due to the combined efforts of Drs. Flom, Safir, and Daugman.
- In 1994, Dr. Daugman was awarded a patent for his automated iris recognition algorithms.
- In 1995, the first commercial products became available.
- In 2005, the broad patent covering the basic concept of iris recognition expired, providing marketing opportunities for other companies that have developed their own algorithms for iris recognition.
- The patent on the IrisCodes implementation of iris recognition developed by Dr. Daugman will not expire until 2011.

3.2 PHYSIOLOGY OF IRIS

The iris, visible through the clear cornea as the colored disc inside of the eye, is a thin diaphragm composed mostly of connective tissue and smooth muscle fibers. It is situated between the cornea
Figure 3.1: Physiology of eye

and the crystalline lens. The color(s), texture, and patterns of each person’s iris are as unique as a fingerprint.

The iris is formed of a trabecular meshwork (elastic connective tissue which gives the appearance of dividing the iris in a radial fashion), layers of pigment, muscle and ligaments, and it controls the amount of light that enters the eye by allowing the pupil to dilate. Color is not used in iris recognition technology. Instead, the other visible features such as the connective tissue, cilia, contraction furrows, crypts, rings and corona distinguish one iris from another.

By the time a human is about eight months old, the iris structures are complete, and they do not change in later life. During the development of the iris, there is no genetic influence on it, a process known as chaotic morphogenesis that occurs during the seventh month of gestation, which means that even identical twins have differing irises. The iris has in excess of 266 degrees of freedom, i.e. the number of variations in the iris that allow one iris to be distinguished from another. The fact that the iris is protected behind the eyelid, cornea and aqueous humour means that, unlike other biometrics such as fingerprints, the likelihood of damage and/or abrasion is minimal. The iris cannot be surgically altered without damage to a person’s vision, and its physical response to light provides one test that prevents artificial duplication of the organ. As with a fingerprint, the iris has a random structure of minutiae or points of detail that can be encoded to form a distinctive template. No two irises are alike, even if they are from identical twins or the left and right eye in the same person. The use of glasses or contact lenses (coloured or clear) has little effect on the representation of the iris and hence does not interfere with the recognition technology.
Chapter 4

HOW IRIS RECOGNITION WORKS

The process of capturing an iris into a biometric template is made up of 3 steps:

1. Capturing the image
2. Defining the location of the iris and optimising the image
3. Storing and comparing the image.

4.1 Capturing the Image :

First, an image must be captured by a camera. A Charge Coupled Device (CCD) camera is used and must be compliant with ANSI/IESNA RP-27.1-96 and IEC 60825-1 standards for radiation and laser products. The subject is 5 inches to 2 feet away from the camera and looks at a LED guide to ensure that the camera focuses on the iris.

Figure 4.1: An IriScan model 2100 iris scanner
4.2 Defining the Location of the Iris and Optimising the Image

Once the camera has located the eye, the iris recognition system then identifies the image that has the best focus and clarity of the iris. Given an eye image, first the pupil is detected and its center is determined. A simple threshold technique is used for pupil detection as its intensity is different from the others. An edge operation is applied to detect a pupil region. By prior knowledge of the pupil shape, a circle is fitted onto the obtained edge information. The iris inner boundary and its center can then be defined by the fitting parameters. The obtained center position is used as a reference point of the following processes. Iris localization is used to locate the inner and outer boundaries of an iris. The inner boundary can be found by detecting a pupil area where its perimeter designates the inner boundary of the iris. The iris outer boundary is a circular edge separating the iris from the sclera zone. Iris edge point detection means to find some points on the inner and outer boundary of iris. The average gray value of pupil is the minimum and that of sclera is the maximum, and the average value of iris is between them. Therefore, on the iris inner and outer boundaries the edge intensity of a pixel must be a maximum. Both boundaries can be located by utilizing intensity differences among organs (pupil, iris, and sclera) and circular shape of the pupil and iris.

The iris recognition system then identifies the areas of the iris image that are suitable for feature extraction and analysis. This involves removing areas that are covered by the eyelids, any deep shadows and reflective areas.
4.3 Storing and comparing the image

The patterns are then encoded using 2D Gabor wavelet demodulation to create a phase code that is similar to a DNA sequence code. 2048 bits of data plus 2048 masking bits are used to produce a 512-byte IrisCode. About 250 degrees of freedom or independent dimensions of variability are represented in the IrisCode. In order to enroll a person for future identification, the IrisCode is stored in a database or on a smart token. When a comparison is required the same process is followed but instead of storing the record it is compared to all the IrisCode records stored in the database. The comparison also doesn’t actually compare the image of the iris but rather compares the hexadecimal value produced after the algorithms have been applied.

In order to compare the stored IrisCode record with an image just scanned, a calculation of the Hamming Distance is required. The Hamming Distance is a measure of the variation between the IrisCode record for the current iris and the IrisCode records stored in the database. Each of the 2048 bits is compared against each other, i.e. bit 1 from the current IrisCode and bit 1 from the stored IrisCode record are compared, then bit 2 and so on. Any bits that don’t match are assigned a value of one and bits that do match a value of zero. Once all the bits have been compared, the number of non-matching bits is divided by the total number of bits to produce a two-digit figure of how the two IrisCode records differ. For example a Hamming Distance of 0.20 means that the two IrisCode differ by 20%.
Chapter 5

HAMMING DISTANCE( A test of statistical independence)

The key to iris recognition is the failure of a test of statistical independence, which involves so many degrees-of-freedom that this test is virtually guaranteed to be passed whenever the phase codes for two different eyes are compared, but to be uniquely failed when any eyes phase code is compared with another version of itself.

The test of statistical independence is implemented by the simple Boolean Exclusive-OR operator (XOR) applied to the 2,048 bit phase vectors that encode any two iris patterns, masked (ANDed) by both of their corresponding mask bit vectors to prevent non-iris artifacts from influencing iris comparisons. The XOR operator detects disagreement between any corresponding pair of bits, while the AND operator ensures that the compared bits are both deemed to have been uncorrupted by eyelashes, eyelids, specular reflections, or other noise. The norms of the resultant bit vector and of the ANDed mask vectors are then measured in order to compute a fractional Hamming Distance (HD) as the measure of the dissimilarity between any two irises, whose two phase code bit vectors are denoted codeA, codeB and whose mask bit vectors are denoted maskA, maskB:

\[ HD = \frac{(\text{code A} \oplus \text{code B}) \cdot \text{mask A} \cdot \text{mask B}}{(\text{mask A} \cdot \text{mask B})} \]  

The denominator tallies the total number of phase bits that mattered in iris comparisons after artifacts such as eyelashes and specular reflections were discounted, so the resulting HD is a fractional measure of dissimilarity; 0 would represent a perfect match. The Boolean operators and are applied in vector form to binary strings of length up to the word length of the CPU, as a single machine instruction. Thus for example on an ordinary 32-bit machine, any two integers between 0 and 4 billion can be XORed in a single machine instruction to generate a third such integer, each of whose bits in a binary expansion is the XOR of the corresponding pair of bits of the original two integers. This implementation of equation(1) in parallel 32-bit chunks enables extremely rapid comparisons of iris codes when searching through a large database to find a match. On a 300 MHz CPU, such exhaustive searches are performed at a rate of about 100,000 irises per second.

The results of a test determining the Hamming distances of independent iris templates are illustrated in Figure below.
If a similar test was conducted comparing templates created from the same iris, the peak would be shifted left to the lower score zone, since the alike templates are less likely to fail tests of statistical independence. A graph illustrating the Hamming distances of pairs of templates created from the same irises is shown in Figure below. The Hamming distance that qualifies two templates as matching depends on where the decision threshold is set. From the Figure, it is clear that a threshold set at 0.35 would correctly assign matches to most comparisons of templates of the same iris, and assign non-matches to comparisons of independent templates.
Figure 5.1: Binomial distribution for 9.1 million cross-comparisons of independent iris templates. Hamming distances center at 0.5. [John Daugman, Cambridge University 2002]
Figure 5.2: Distribution of Hamming distances for template comparisons. The left peak is composed of comparisons of matching pairs of templates. [John Daugman, Cambridge University 2002]
5.1 Probabilities of FAR and FRR with Iris Recognition

There are two error rates that need to be taken into consideration. False Reject Rate (FRR) occurs when the biometric measurement taken from the live subject fails to match the template stored in the biometric system. False Accept Rate (FAR) occurs when the measurement taken from the live subject is so close to another subject’s template that a correct match will be declared by mistake. The point at which the FRR and the FAR are equal is known as the Crossover Error Rate (CER). The lower the CER, the more reliable and accurate the system. In iris recognition technology, a Hamming Distance of .342 is the nominal CER. This means that if the difference between a presented IrisCode record and one in the database is 34.2% or greater then they are considered to have come from two different subjects. During recognition mode, this comparison has to occur between the IrisCode record from the live subject and every IrisCode stored in the database before the live subject is rejected.

The following table shows the probabilities of false accept and false reject with iris recognition technology:

<table>
<thead>
<tr>
<th>Hamming Distance</th>
<th>False Accept Probability</th>
<th>False Reject Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>.28</td>
<td>1 in 10^{12}</td>
<td>1 in 11,400</td>
</tr>
<tr>
<td>.29</td>
<td>1 in 10^{11}</td>
<td>1 in 22,700</td>
</tr>
<tr>
<td>.30</td>
<td>1 in 6.2 billion</td>
<td>1 in 46,000</td>
</tr>
<tr>
<td>.31</td>
<td>1 in 665 million</td>
<td>1 in 95,000</td>
</tr>
<tr>
<td>.32</td>
<td>1 in 81 million</td>
<td>1 in 201,000</td>
</tr>
<tr>
<td>.33</td>
<td>1 in 11 million</td>
<td>1 in 433,000</td>
</tr>
<tr>
<td>.34</td>
<td>1 in 1.7 million</td>
<td>1 in 950,000</td>
</tr>
<tr>
<td>.342</td>
<td>1 in 1.2 million</td>
<td>1 in 1.2 million</td>
</tr>
<tr>
<td>.35</td>
<td>1 in 295,000</td>
<td>1 in 2.12 million</td>
</tr>
<tr>
<td>.36</td>
<td>1 in 57,000</td>
<td>1 in 4.84 million</td>
</tr>
<tr>
<td>.37</td>
<td>1 in 12,300</td>
<td>1 in 11.3 million</td>
</tr>
</tbody>
</table>

5.2 SPEED PERFORMANCE

On a 300 MHz Sun workstation, the execution times for the critical steps in iris recognition are as follows, using optimized integer code:

<table>
<thead>
<tr>
<th>OPERATION</th>
<th>TIME</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assess image focus</td>
<td>15 msec</td>
</tr>
<tr>
<td>Scrub specular reflections</td>
<td>56 msec</td>
</tr>
<tr>
<td>Localize eye and iris</td>
<td>90 msec</td>
</tr>
<tr>
<td>Fit pupillary boundary</td>
<td>12 msec</td>
</tr>
<tr>
<td>Detect and fit both eyelids</td>
<td>93 msec</td>
</tr>
<tr>
<td>Removes lashes and contact lens edges</td>
<td>78 msec</td>
</tr>
<tr>
<td>Demodulation and Iris code creation</td>
<td>102 msec</td>
</tr>
<tr>
<td>XOR comparison of 2 iriscodes</td>
<td>10 s</td>
</tr>
</tbody>
</table>
Chapter 6

ADVANTAGES AND DISADVANTAGES OF IRIS RECOGNITION

Though iris recognition is believed to be one of the most secure biometric technology available due to reliability, ease of use, and software and hardware devices that currently support it. The algorithms developed for iris recognition have been well tested and perform well when implemented on today's computer hardware. But since it is relatively new technology some problems are witnessed which are being worked upon. Here is an overview of pros and cons of iris recognition system.

6.1 ADVANTAGES OF IRIS RECOGNITION

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) that 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 0.2% of the human population who have a genetically identical twin.

• An iris scan is similar to taking a photograph and can be performed from about 10cm 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 fingerprint 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).

- It is non-invasive, as it does not use any laser technology, just simple video technology. The camera does not record an image unless the user actually engages it.

- It poses no difficulty in enrolling people that wear glasses or contact lenses.

- Proven highest accuracy: iris recognition had no false matches in over two million cross-comparisons, according to Biometric Product Testing Final Report (19 March 2001, Center for Mathematics and Scientific Computing, National Physics Laboratory, U.K.)

- 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.

- It would only take 1.7 seconds to compare one million IrisCodes on a 2.2GHz computer.

### 6.2 DISADVANTAGES OF IRIS RECOGNITION

- 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. However, several academic institutions and biometric vendors are developing products that claim to be able to identify subjects at distances of up to 10 meters ("standoff iris" or "iris at a distance").

- The iris is a very small organ to scan from a distance. It is a moving target and can be obscured by objects such as the eyelid and eyelashes. Subjects who are blind or have cataracts can also pose a challenge to iris recognition, as there is difficulty in reading the iris.

- As with other photographic biometric technologies, iris recognition is susceptible to poor image quality, with associated failure to enroll rates.

- The camera used in the process needs to have the correct amount of illumination. Without this, it is very difficult to capture an accurate image of the iris. Along with illumination comes the problem with reflective surfaces within the range of the camera as well as any unusual lighting that may occur. All of these impact the ability of the camera to capture an accurate image. The system linked with the camera is currently only capturing images in a monochrome format. This results in problems with the limitations of greyscale making it difficult to distinguish the darker iris colourations from the pupil.
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.
Chapter 7

COMPARISON WITH OTHER BIOMETRIC SYSTEMS

Three factors can be used for security: something you know (password or PIN), something you have (smart token or access card), and something you are (biometric). Biometrics can be used alone or in conjunction with one of the other factors to strengthen the security check. Biometric technology has advantages over both of the other factors in that the user does not need to remember anything or possess a physical token in order to be identified. Tokens and cards can be lost, and passwords and PINs can be forgotten or compromised. A biometric is only susceptible to forgery, which can be extremely difficult, depending on the biometric.

Iris recognition falls into the physical biometric category as opposed to behavioral biometrics such as signatures. Other physical biometric technologies include fingerprinting, retinal scanning, speaker recognition, facial scanning and hand geometry. The National Center for State Courts (NCSC) published information comparing these physical biometric methods. The NCSC data is substantiated by a similar comparison table found at the IEEE Computer Society. Here are some highlights from both groups findings.

7.1 IRIS RECOGNITION vs FINGERPRINT

Fingerprint recognition is widely accepted by civil law enforcement and forensic government applications (the AFIS database); as such, fingerprints are excellent for background checks. It has wide range of vendors and solutions and the ability to enroll multiple fingers.

- But fingerprint is not as accurate as iris recognition. Fingerprint false accept rate varies by vendor, and is approximately 1 in 100,000. whereas Iris recognition false accept rate is 1 in 1.2 million statistically.
- Most high-end fingerprint systems measure approximately 40-60 characteristics; iris recognition looks at about 240 characteristics to create the unique IrisCode.
• Iris recognition can perform 1: all matches in a high speed environment, whereas fingerprint searches take much longer, may require filtering, and may return multiple candidate matches.

• The long association of fingerprints with criminals makes this biometric an uncomfortable method of authentication for some people.

• Most systems require physical contact with a scanner device that needs to be kept clean (hygiene issue).

• The large number of players (different algorithms) means no fingerprint standards exist. Iris recognition has one core standard, which is flexible and open to all partners, and has been the foundation for Oki, Panasonic and LG hardware solutions.

• Based on occupation, trauma or disease, individual fingerprints may be obscured, damaged or changed meaning some people may need to enroll multiple times over the course of their lives. Fingerprint readability also may be affected by the work an individual does. For example, transportation workers such as mechanics, food workers, or maintenance workers may present fingerprints that are difficult to read due to dryness or the presence of foreign substances, such as oil or dirt, on fingers.

7.2 IRIS RECOGNITION vs HAND GEOMETRY

Hand Geometry is currently being used for functions such as access control, employee time recording and point of sale applications. It is fairly easy to use and has reasonably high acceptance among users, and it is opt-in.

• Iris recognition can perform 1: all matches in a high speed environment, whereas hand geometry does not support 1: all matching with large databases.

• The error rate for hand geometry is 1 in 500 compared to 1 in 131,000 for iris recognition.

• Hand size and geometry changes over time, especially in the very young and the very old whereas The iris itself is stable throughout a persons life (approximately from the age of one); the physical characteristics of the iris don't change with age.

• People are reluctant to place hand where many others have touched so hygiene is another issue with hand geometry, whereas in iris recognition there is no physical contact of person with camera.

• Also extreme sizes are not accommodated in all hand readers.

7.3 IRIS RECOGNITION vs FACIAL RECOGNITION

Facial recognition is effective for surveillance applications. It provides a first level scan within an extremely large, low-security situation. It is easy to deploy, can use standard CCTV hardware integrated with face recognition software. It is a Passive technology, does not require user cooperation and works from a distance.
• lighting, age, glasses, and head/face coverings all impact false reject rates in facial recognition whereas iris recognition poses no difficulty in enrolling people that wear glasses or contact lenses.

• Face recognition has Privacy concerns: people do not always know when their picture/image is being taken and being searched in a database or worse, being enrolled in a database whereas in Iris Recognition subjects agree to enroll and participate, reducing privacy concerns.

• Iris recognition is more reliable than facial recognition.

• The NPL study cites a false accept rate of 1:100 for facial recognition versus 1:1.2 million for iris recognition.

7.4 IRIS RECOGNITION vs RETINA RECOGNITION

Retinal scanning is often confused with iris recognition, but they are very different biometric technologies. The retina is located at the back of the eye and contains distinctive vascular patterns that can be used for identification and verification. Retinal scanning is the only biometric that is more reliable than iris recognition.

• The error rate for retinal scanning is 1:10,000,000 compared to the iris recognition error rate of 1:131,000.

• The retinal scanning process is different from iris recognition and does not involve an IrisCode.

• Both retinal and iris technologies are extremely accurate and reliable and have very low false acceptance rates.

• Opinions seem to differ on which feature, iris or retina, is more reliable to use throughout life. According to John Marshall of Retinal Technologies, The iris is harder to map as an image because it fluctuates based on the size of the pupil, and drug or medicinal use, and age. The retina stays constant throughout your life, unless you have glaucoma or diabetes. True, the iris is not fully shaped until about eight months of age, but after that age, it is commonly believed to be stable.

• A retinal scanning subject must stay very still, with the eye at a distance of no more than 3 inches from the scanner, whereas iris recognition can be accomplished with the subject at a distance of up to about 2 feet from the camera.

• People wearing glasses must remove them for a retinal scan. For iris recognition, the National Physical Laboratory (NPL) tests found that glasses can make enrollment more difficult, but they can remain in place for verification without causing difficulty.

• The NPL tests revealed difficulty in enrolling a blind persons iris because the system required both eyes to be enrolled. Depending upon the nature of the blindness, enrollment of two eyes using retinal scanning might also be prohibitive. No NPL data was reported for retinal scans of blind eyes.
Neither technology has been inexpensive in the past, but recent developments are bringing prices down for both iris recognition and retinal scanning. Retinal scans are probably most appropriate for applications that require the highest levels of security, where the subject is very cooperative and patient, or is required by law to succumb to the scan.
Chapter 8

APPLICATIONS OF IRIS RECOGNITION

Iris recognition systems are being used today to control physical access, to facilitate identity verification and for computer authentication. Real-world iris recognition applications have been implemented for airport and prison security, automatic teller machines, authentication using single sign-on, to replace ID cards, and to secure schools and hospitals. This section describes some of the widely used commercial applications using the iris recognition technology for controlling and monitoring physical secure access to restricted areas and resources.

8.1 IrisAccess 2200T System

Iridian Technologies and LG Electronics have teamed up together to create the IrisAccess 2200T system. The system is used to identify and authenticate user access to physical areas. The system designed and developed using Iridian Technologies Iris recognition software and LG’s imaging platforms delivers superb accuracy, speed, scalability and convenience for user identification and authentication.

Some of the features of the IrisAccess 2200T system are summarized below:

The imaging device automatically detects that a subject is approaching. The individual has to glance at the imaging device from a distance of 310 inches, which captures the iris image and digitally processes it to form a 512 byte IrisCode template.

A patented search function enables real time database matching at remote unit level. User access is granted immediately as soon as the presented IrisCode matches a valid IrisCode template in the database.

Using organization Intranet and encrypted transaction, TCP/IP communication, the system can control the access to the secure area within the organization and up to 254 doors over the Internet. Other features include audio interface in multiple languages, non-intrusive, one to many search identification and optional verification mode.
8.2 *EyePass*™ System

The *EyePass*™ System developed by EyeTicket Corporation is primarily aimed at aviation industry. It is an access control service provided to air carriers, airport authorities and other large employers. Some of the features of the *EyePass*™ system are:

- Access control to secure areas for pilots, flight crews and ground staff at airports and corporate installations.
- Time and attendance functions are automated and secured by the system.

8.3 *JetStream*™ System

The *JetStream*™ System also developed by EyeTicket Corporation is used for positively identifying and authenticating passengers traveling on airlines. It is used in conjunction with the airlines reservation system.

Some of the features of the *JetStream*™ system are:

1. Simplifies and expedites transactions providing maximum security and risk management at a competitive cost
2. Allows passengers to check in and board an aircraft simply by using ones iris.

The *JetStream*™ system is a fully developed proven solution currently deployed at London Heathrow Airport. Other application areas using the *JetStream*™ system include immigration control, railways and hotel industry.

8.4 Information Security :

This section describes a commercially available application based on the iris recognition technology that addresses the issues of password management and uses ones iris as a positive identity to authenticate the access to data and information.

8.4.1 *PanasonicAuthenticam*™

Iridian Technologies and Panasonic have teamed up to design and develop a system that primarily addresses issues related to passwords, PINs and token cards. *PanasonicAuthenticam*™ enabled with unique Private *Id*™ software from Iridian Technologies allows the iris recognition camera to capture, select and secure iris images. Some of the important features of the system are summarized below.

*PanasonicAuthenticam*™ enables system administrators to secure access to personal computers, files, folders, and applications only to authorized users. It uses the Private *ID*™ software, which generates IrisCode compatible with *KnoWho*™ Authentication Server from Iridian Technologies. Also, it includes the I/O software SecureSuite™, which allows multiple users to securely access restricted resources. The cost associated with password management and the risks of fraudulent activities are substantially reduced.
8.4.2 Authentication Server

The KnoWho™ Authentication Server from Iridian Technologies is designed to integrate with mission critical applications, transaction systems, network environments that require high performance authentication capabilities. The authentication server is a major component used to store IrisCode templates and to process the authentication. The Authentication server has two main functions, first to store IrisCode templates and second a processing engine that performs real-time matching. The KnoWho™ Software Development Kit (SDK) allows customization of the Authentication server capabilities for other applications.

Some of the features of the KnoWho™ Authentication Server are 20:

- Identification/ Recognition: one-to-many matching.
- Verification: one-to-one matching.
- Ability to enroll, update and delete new and existing IrisCode templates, data etc.
- Use of Oracle 8i and SQL Server RDBMS to store IrisCode and related data.
- Compatible with PrivateID™ supported cameras such as Panasonic™ Authenticam™.
- Data encryption at database level.
- 45 Option to store facial images.
Chapter 9

CONCLUSION

Based on the applications, reliability, ease of use, and software and hardware devices that currently support it, iris recognition technology has potential for widespread use. Iris recognition costs compare favorably with many other biometric products on the market today. Iris recognition is the most secure biometric technology available.

Iris recognition removes the need for physical contact with the biometric recording device and is recommended for both verification and identification. The algorithms developed for iris recognition have been well tested and perform well when implemented on today’s computer hardware. So why are there not iris recognition devices in every airport, at every bank’s ATM and at every server and workstation? For computer login, cost and portability may be factors. Even though a camera and software can be purchased today for $239.00,57 the costs add up when a device must be added to each workstation. The cameras, while small, are still more bulky than a workstation fingerprint reader and would probably be cumbersome to carry around to facilitate logging in to a laptop. On the other hand, the ability to use an iris recognition camera as a video conferencing device may make up for the cameras’ bulk, and makes iris recognition a more attractive biometric authentication choice for standard desktop configurations.

For ATMs at banks, iris recognition seems to be the perfect biometric. However, it will take longer to enroll customers using a biometric device than it does to simply assign and change a PIN. Since cards with PIN are already in use, it may be a while before any type of biometric device becomes prevalent in the banking industry. The beauty of iris recognition, however, is that it is non-intrusive and very secure, and it could eliminate the need for a card for ATM transactions. This could drastically reduce the effects of credit card theft because the cards would be useless at the ATM. Secure banking that relies on who you are rather than what you have would certainly be convenient.

The increase in requirements for securing airports could drive up the use of biometric devices for transportation security. Since there were not many identification/verification systems in airports prior to September 11, 2001, the opportunity is ripe to install state-of-the-art identification systems for travelers. Iris recognition systems seem to fill that need well, and there is already evidence that the transportation industry recognizes the usefulness of iris recognition. Terrorist activity increases the need for secure access to restricted areas, so there may also be increases in installation of biometric devices for building entry. In addition to its reliability, the lack of physical contact required for verification may make iris recognition more attractive to the general public than fingerprint or hand geometry biometric devices.
Iris recognition has made great strides in the last 5 years. It scores well compared to the other biometric technologies, both in ease of use and in reliability. Perhaps someday, iris recognition will be prevalent for many more applications.
Bibliography


