Report on the
Literature Study of Iris Biometric Recognition

Jonas Nyasulu Tierry Fomene
jonny834@student.liu.se thifo867@student.liu.se
Supervisor: Vivieke Fåk
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

This report discusses the use of the iris-based biometric recognition. Biometric recognition is the automated recognition of individuals based on the physiological and behavioral characteristics. The recognition can be positive or negative. It highlights the key areas where the iris biometric method has been used successfully, and what are its shortfalls. It presents an overview of the algorithm used in Iris biometric recognition. It also compares the performance of the Iris biometric method with the other biometric methods in terms of cost-effectiveness, usability, speed and other factors. The iris is very unique in that it has many features such as crypts, furrows and collarettes, which are used by the algorithms for comparison between a template and an image acquired for recognition.

Most of the algorithms used for iris recognition have a very low false acceptance rate compared to the other biometric methods, and these algorithms can do millions of comparisons on easily available hardware.

1. Introduction

Biometrics is the automated measurement of physiological or behavioral characteristics of individuals [1]. Physiological characteristics include face, fingerprints, iris and retinal features, hand geometry, and ears. Behavioral characteristics include handwritten signature, voice, keystrokes (typing), and gait (how a person walks).

Today there are many uses of biometrics each has its own advantages and disadvantages according to the requirements on biometric identifiers. A practical biometric system should have acceptable recognition accuracy, speed with reasonable resource requirements. It should be harmless to users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods [1].

For a long time the fingerprints have been one of the most widely used and accepted biometric. This is evidenced by the Chinese who have used fingerprints to sign documents for over 1000 years [14].

Iris recognition is one of the biometrics that is used for identification and verification due to its accuracy. In a verification system, the system authenticates a person's identity by comparing the captured biometric characteristic with her own biometric template(s) prestored in the system. In an identification system, the system recognizes an individual by searching the entire template database for a match [1]. In this report we will describe the physiology of the iris, the algorithm used in iris recognition, analyze their performance and state some areas that use the iris biometric.

2. Motivation

Something you hold for security, can be lost, something you know like passwords or PIN, can be guessed, or forgot. Biometrics provide an alternative to these methods, or they can be used in combination (multimodal). Fingerprints, which are widely used, can be forged (gummy fingers). The face changes over a period of time, even with the best algorithms face recognition (for faces taken one year apart) has error rates of about 43 to 50 % [9], hand geometry is not distinctive enough to be used in large scale applications, hand-written signatures can be forged. The iris is different for any two individuals even for identical twins, DNA is not unique among identical twins.

Most of the currently deployed commercial algorithms for iris recognition (by John Daugman) have a very low false acceptance rate compared to the other biometric identifiers. Some of the biometric identifiers have problems with replay attacks, for instance fingerprints. Replay attacks with the iris biometric can checked by detecting the liveness of the eye. The pupil changes its size when light is shone into the eye. The algorithms are able to measure this change in pupil size [2]. The process of capturing the iris image is not intrusive. Iris images can be computer matched more accurately than a face image, and it's acknowledged that iris recognition is more accurate than any other biometric technique [8], although there are some concerns regarding enrollment failure rates (capturing the initial iris image to be used as a template for comparing with other images). The failure to enroll rate (FTE) is the rate at which a biometric system fails to enroll a subject's biometric sample. The process of enrolling a subject for the first time requires some training as explained in section 3.1.

These are some of the reasons that make the iris recognition technology suitable for applications in which the user is cooperative.

3. Physiology of the Iris

Figure 1 shows the structure of the iris. Iris scans analyze the features that exist in the colored tissue surrounding the pupil which has more than 200 points that can be used for comparison, including rings, furrows and freckles. The scans use a regular video camera style and can be done further away than a retinal scan. It will work through glasses and contact lenses and in fact has the ability to create an accurate enough measurement [12].

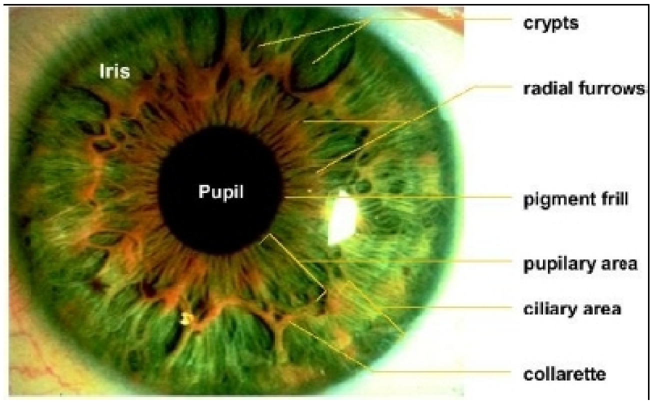

Figure1: Structure of the Iris [15]

4. Enrollment

The iris image is captured using a standard camera using both visible light and infrared light and this can be a manual or automated procedure. In the manual procedure the user needs to adjust the camera to get the iris in focus. This process is more manually intensive and requires proper user training to be successful.

The automatic procedure uses a set of cameras that locate the face and iris automatically thus making the process much more user friendly [4]. 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. The image is then analyzed to identify the outer boundary of the iris where it meets the white sclera of the eye, the pupillary boundary and the centre of the pupil. This results in the precise location of the circular 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, and any deep shadows [4].

5. Algorithm

Iris recognition systems analyze the random pattern of a person's iris [8]. Most commercial iris recognition systems use patented algorithms developed by John Daugman [7]. The algorithms identify the outer boundaries of the iris and the pupil. This is the region that is transformed into bit patterns that are later used for a statistical comparison between a template and an image presented by a user who requires to be verified or identified.

Here is a summary of the algorithm as described by Negin [11].

An iris image captured by a camera is converted into a an IrisCode which is a bar-code like bitstream shown on the top left corner of figure 2.

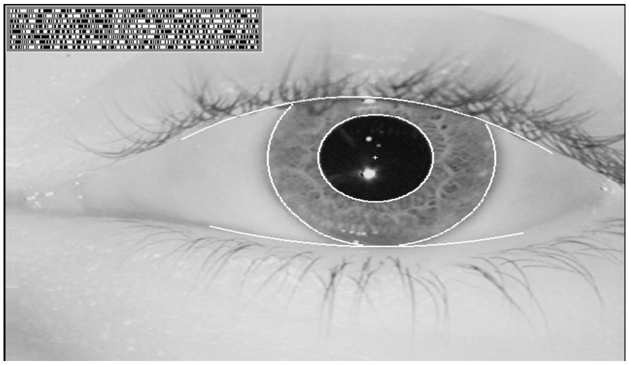

Figure 2: An Iris pattern taken from a distance of about 35cm [9]

The IrisCode is based on information from a set of Gabor wavelets. These wavelets are specialized filter banks that extract information from a signal at a variety of locations and scales. The filters optimize the resolution in both the spatial and the frequency domain. The IrisCode is calculated using eight circular bands that have been adjusted to conform to the iris and pupil boundaries, as shown in Figure 1. IrisCodes derived from this process are compared with previously generated IrisCodes. The number of positions in which the two IrisCodes differ is termed the Hamming distance (HD). For two identical IrisCodes, the HD is zero; for two perfectly unmatched IrisCodes, the HD is 1. For different irises, the average HD is about 0.5, which indicates a 50 percent difference in the codes. For two different images from the same iris, the HD ranges from approximately 0.05 to 0.1, a variation that includes contributions from video noise as well as variations in the position of the user's eye with respect to imaging optics.

Generally, an HD threshold of 0.32 can reliably differentiate authentic users from impostors.

Several methods have been proposed for iris recognition [4], Wildes [10] describes a system for personal verification based on automatic iris recognition.

6. Applications Using the Iris Biometric Recognition Technology

6.1 Banking

Automated Teller Machines (ATM) and Internet banking are vulnerable to fraud. The Iris biometric can be used to address some of the problems related to Internet banking and ATMs.

6.2 Social Welfare

This area has also been affected by fraud whereby individuals try to claim social welfare benefits more than once by using multiple identities. The Iris biometric can be used to minimize this problem.

The CHILD Project - Children's Identification and Location Database [2].

This is nationwide network and registry utilizing iris recognition technology that is used to quickly and positively identify missing children across the United States.

6.3 Border Control / Immigration

The United Arab Emirates (UAE) uses iris recognition on foreigners entering the UAE at 35 air, land, and sea ports. Each traveler is compared against about a million IrisCodes on a watch-list. The time required for an exhaustive search through the database is about 1 second. Billions of comparisons are made each day[13].

Iris Recognition for staff at Manchester Airport. [5]

The Iris is used for access control at the Manchester airport in UK (Heathrow, Manchester, Birmingham, Gatwick). It controls the access of staff to restricted zones in the airport by using access-control portals combined with iris-recognition cameras. The total number of users in this system is about 25,000. This has improved the manual checking procedures previously used at the airport.

IRIS – Iris Recognition Immigration System

The iris has been used at several airports in the UK to clear immigration in a fast and secure way [6].

Enrollment takes about 5-10 minutes and recognition takes about 20 seconds.

7. Performance

The Iris biometric recognition is used due to its unicity and performance. As already indicated the method has a very low false acceptance, it's not possible to find two different people with the same iris features, even with twins. The iris characteristics don't change with age. This technique uses a very strong algorithm for verification and identification. Table 1 shows the performance of the iris method using the Daugman algorithm. The tests were done by several independent organizations.

Testing Organizations	Number of Cross Comparisons	False Matches
Sandia Labs, USA (1996)	19,701	0
British Telecom Labs,UK (1997)	222,743	0
Sensa Corp, USA (2000)	499,500	0
Joh.Enschede, NL (2000)	19,900	0
EyeTicket, USA (2001)	300,000	0
National Physical Lab, UK (2001)	2.73 million	0
J. Daugman, UK (2003)	9.1 million	0
Iridian Technologies, USA (2003)	984 million	0

Table 1: Tests of the Daugman Iris Recognition Algorithms [3].

Table 1 shows that all the tests that have been carried out have a false match rate of zero. This makes the iris recognition suitable for many authentication systems. It has a false rejection rate of 1 in 1.2 million. False rejection is a measure of authenticated users who are rejected.

Method	Coded Pattern	Mis-identification rate	Security	Application
Iris Recognition	Iris pattern	1/1200000	High	High security facilities
Finger printing	Fingerprints	1/1,000	Medium	Universal
Hand Shape Size,	Length and thickness of hands	1/700	Low	Low-security facilities
Facial Recognition	Outline, shape and distribution of eyes and nose	1/100	Low	Low-security facilities
Signature	Shape of letters, writing order, pen pressure	1/100	Low	Low-security facilities
Voice printing	Voice characteristics	1/30	Low	Telephone service

Table 2: Technology Comparison of various biometrics [18]

Table 2 show that the false rejection (Mis-identification rate) of the iris recognition method is the lowest among all the biometrics.

Iris recognition requires reasonably controlled and cooperative user interaction. In applications where user interaction is frequent , the technology is easier to use, however in applications where user interaction is infrequent (e.g. national ID, driving licenses) there may be some ease-of-use issues [12].

The cost of the camera for iris recognition is reasonably expensive compared to devices used by the other biometrics. For instance a random search for one of cheapest low-cost cameras for iris recognition (Panasonic Authenticam) revealed that it costs 5 times more than a fingerprint reader (Microsoft fingerprint reader). To implement iris recognition requires a computer and an adjustable camera that can accommodate people of different heights. This can be more costly on large scale compared with encoded cards, or fingerprints.

8. Future Perspective

The biometric market is growing each year as shown in figure 3.

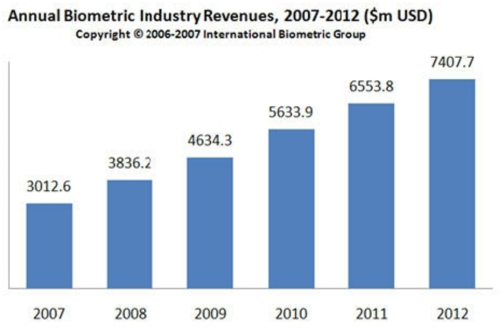

Figure 3: The Annual Biometric Industry Revenues [16]

Figure 4 shows that the iris recognition has a smaller percentage (~ 5 %) when compared with other biometric technologies. Partly this has to do with the cost of equipment needed. This percentage is expected to grow since cases of identity theft and online fraud are increasing and this has resulted in an increase for the need of more powerful recognition systems. So iris recognition will be worth the cost. This is evidenced by the increased attention shown to Iris recognition due to its high reliability [17].

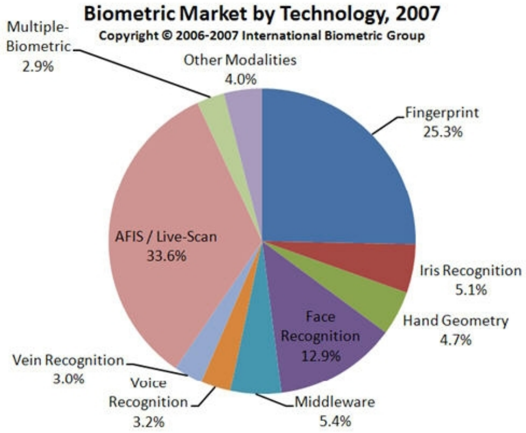

Figure 4: The Biometric Market by Technology [16]

9. Related Work.

Miyazawa [19] describes an algorithm for iris recognition using phase-based image matching which they used in commercial fingerprint verification units. They propose that their approach can be highly useful for multimodal biometric system having iris and fingerprint recognition capabilities.

10. Conclusion.

The iris biometric recognition method can be used to improve business processes since the algorithms used have a very low false acceptance rate, and are very accurate. The comparisons are made for a few seconds. The iris recognition algorithms are best suited for applications where subjects are willing to go through enrollment and verification. This method can be used in banking applications to authenticate users who wish to carry out some online transactions. The user can have a camera similar to a webcam which can take the iris image to be used for authentication. ATMs could also be fitted with the same camera device.

The iris biometric method is already being used in identification and authentication in many UK airports and the UAE.

The effectiveness of the iris biometric method can be much higher if used in combination with other biometrics (to be multimodal), or used in combination with a password/PIN, or token. This can also address the limitation of the iris method for users who are blind, or whose irises are affected some eye disease (drooping eyelids, cataracts etc).

Replay attacks in the iris biometric method is checked by detecting liveness of the eye (iris). Some algorithms have been developed that are used to check the liveness of the iris (variations in pupil size when there is change of light), and they also have a low false acceptance rate.

References

[1] D. Maltoni et. al, Handbook of Fingerprint Recognition (2003)
http://bias.csr.unibo.it/maltoni/handbook/chapter_1.pdf

[2] The Child Project™
http://www.thechildproject.org/

[3] Tests of the Daugman Iris Recognition Algorithms
http://www.cl.cam.ac.uk/~jgd1000/iristests.pdf

[4] Aboul Ella Hassanien and Jafar M.Ali, "An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory", Advanced Modeling and Optimization journal, Volume 5, Number 2, pp. 93-104, 2003

[5] Manchester Airport launches staff biometrics (January 2008)
http://news.zdnet.co.uk/security/0,1000000189,39292344,00.htm

[6] The Iris Recognition Immigration System (IRIS)
http://www.iris.gov.uk

[7] Libor Masek, Recognition of Human Iris Patterns for Biometric Identification (2003),
http://www.csse.uwa.edu.au/~pk/studentprojects/libor/LiborMasekThesis.pdf

[8] Douglas Walker IMAGE RECOGNITION BIOMETRIC TECHNOLOGIES MAKE STRIDES (2006)
www.ncsconline.org/WC/Publications/Trends/2006/DocManBiometricsTrends2006.pdf

[9] John Daugman, "How Iris Recognition Works", IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004,pp 21-30

[10] R. Wildes, "Iris Recognition: An Emerging Biometric Technology" Proceedings of the IEEE, vol.85, no.9, September 1997
http://ieeexplore.ieee.org/iel3/5/13673/00628669.pdf

[11] M. Negin et al., "An iris biometric system for public and personal use", IEEE Computer Volume 33, Issue 2, pp 70 – 75, Feb. 2000

[12] Individual Biometrics – Iris Scan
http://ctl.ncsc.dni.us/biomet%20web/BMIris.html

[13] John Daugman, Iris recognition border-crossing system in the UAE, 2004
http://www.cl.cam.ac.uk/~jgd1000/UAEdeployment.pdf

[14] Max Chasse, La Biometrie au Quebec, Les enjeux, july 2002
http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf

[15] Structure of the Iris,
http://pagespersoorange.fr/fingerchip/biometrics/types/iris.htm

[16] The International Biometric Group,
http://www.biometricgroup.com/reports/public/market_report.html.

[17] J. G. Daugman. High confidence visual recognition of persons by a test of statistical independence. IEEE Trans. On PAMI, 15(11):1148–1161, 1993.

[18] AIM Japan, Automatic Identification Seminar, Sept.14, 2001
http://www.biometricsinfo.org//irisrecognition.htm

[19] Kazuyuki Miyazawa et al., A Phase-Based Iris Recognition Algorithm (2006)
http://www.aoki.ecei.tohoku.ac.jp/~miyazawa/icip2006.pdf