VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

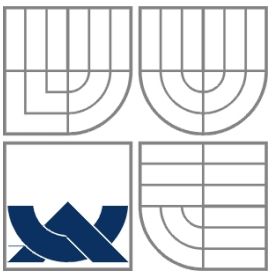
FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

EVALUATION OF BIOMETRIC SYSTEM - EYE IRIS TECHNOLOGY

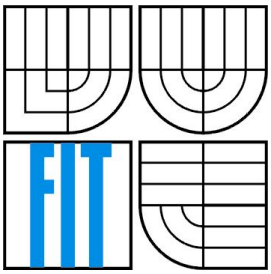
BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE LUBOŠ MLČOCH
AUTHOR

BRNO 2010



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
ÚSTAV INTELIGENTNÍCH SYSTÉMŮ

FACULTY OF INFORMATION TECHNOLOGY
DEPARTMENT OF INTELLIGENT SYSTEMS

EVALUACE BIOMETRICKÉHO SYSTÉMU - TECHNOLOGIE DUHOVKY OKA

EVALUATION OF BIOMETRIC SYSTEM - EYE IRIS TECHNOLOGY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

LUBOŠ MLČOCH

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. PETR DITTRICH

BRNO 2010

Abstrakt

Tato práce stručně popisuje základní pojmy z oblasti biometrie, historii biometrie, biometrický systém a jeho vlastnosti. Dále pojednává o základních principech technologie rozpoznávání podle duhovky oka. Také jsou popsány testy provedené na několika různých systémech rozpoznávání podle duhovky oka a nakonec jsou shrnuty dosažené výsledky.

Abstract

This thesis briefly describes basic biometric terms, a brief history of biometrics, biometric system and its performance and characteristics. Basic principles of iris recognition technology are also discussed. Finally, this thesis describes tests performed on various iris recognition systems and sums up the results.

Klíčová slova

biometrie, oko, duhovka, rozpoznávání duhovky, evaluace, OKI IrisPass, Iridio myš, Panasonic Authenticam, VeriEye, MATLAB, testy výkonnosti

Keywords

biometrics, eye, iris, iris recognition, evaluation, OKI IrisPass, Iridio mouse, Panasonic Authenticam, VeriEye, MATLAB, performance tests

Citace

Luboš Mlčoch: Evaluation of biometric system – eye iris technology, bakalářská práce, Brno, FIT VUT v Brně, 2010

Evaluation of biometric system – eye iris technology

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením Ing. Petra Dittricha. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

……
Luboš Mlčoch
3.5.2010

Acknowledgements

I would like to thank my supervisor Ing. Petr Dittrich for his advice and help. I also wish to thank my parents for their support over the years.

© Luboš Mlčoch, 2010
Tato práce vznikla jako školní dílo na Vysokém učení technickém v Brně, Fakultě informačních technologií. Práce je chráněna autorským zákonem a její užití bez udělení oprávnění autorem je nezákonné, s výjimkou zákonem definovaných případů.

Contents

1 Introduction

In today's world biometric technologies are common and can be seen in many various locations – airports, entertainment parks, internet data centers, casinos or even sport stadiums. Law enforcement organizations have been using biometric technologies for quite some time now – to recognize repeat offenders, solve criminal cases or identify dangerous persons. With the ever growing need for secure and efficient security systems, biometrics is becoming more and more popular. Unlike the standard identification card, personal identification number or password that we use every day to access a building, room, or just to log in to our bank account, a biometric trait can not be lost or forgotten and most of them can not be easily stolen either. Nowadays, various biometric technologies are built in to notebooks, palmtops or even USB drives. Most of the biometric technologies provide a very secure and efficient security solutions, while maintaining easy and convenient usage. Many of these new and automated biometric systems are based on ideas that were conceived a long time ago.

In my opinion, one of the most interesting biometric technologies is the iris recognition technology. The human iris is a very unique biometric. No two irides are alike. That characteristic alone would make the iris a solid biometric, but the iris is also very stable, formed before the birth, and not changing at all throughout human life. Although the iris is accessible, and can be easily seen and captured, which makes the collection relatively easy, it is a highly protected organ. Iris also boasts with large inter-class variability and small intra-class variability, that means there is a distinct difference between individuals, but very small difference between samples taken from one particular individual. All these characteristics make iris a great biometric.

The iris recognition is generally regarded as one of the most reliable and robust form of biometric authentication. It has been successfully deployed in large-scale systems. On the other hand, most of the published results were recorded under favorable conditions and there are not many independent tests of the technology. This thesis is devoted to testing various iris recognition devices and software.

Chapter **2** describes what biometrics means, then a brief history of biometrics follows. The next part is devoted to verification and identification. Biometric system, its characteristics, performance and some of the possible errors are mentioned as well.

In chapter **3**, the human iris and its characteristics are discussed. Both advantages and disadvantages of using iris recognition technology are mentioned as well.

Chapter **4** is devoted to all iris recognition devices and software that have been tested. Each device and software, is briefly described and my personal experience with them is mentioned as well.

Chapter **5** describes performed tests and achieved results.

In chapter **6** findings and suggestions for future work are presented .

2 Biometrics

2.1 The term biometrics

The term **biometrics** comes from ancient Greek *bios* = “life“ and *metros* = “measure“ [1]. Biometrics is generally considered to be the study of measurable biological characteristics. In the field of computer science, it refers to authentication techniques that rely on measurable physical characteristics that can be automatically checked.

Although biometric technology has various uses, its primary purpose is to provide a much more secure alternative to the traditional access-control systems used to protect either corporate or personal assets. Many of the problems that biometrics help to solve are the weaknesses present in current access-control systems. Weak passwords, shared credentials or loss of a key or card are the most common problems. Biometrics can solve all these problems by requiring an additional credential – something associated with the persons's own body – before granting access to a computer system, room or building.

Thanks to significant advancements in the field of computer processing over the last few decades, automated biometric systems have become available. Although it must be noted, that many of these new automated techniques are based on ideas that were originally conceived many years ago.

2.2 A brief history of biometrics

One of the oldest and most basic examples of a characteristic that humans use for recognizing each other is the face. Since the very beginning of civilization, humans have used faces to identify known and unknown individuals. At first, it was a very simple task, but as the world developed and human population increased, and better and more efficient methods of travel became available, this task has become increasingly challenging and difficult. The concept of human to human recognition can be also seen in behavioral biometrics, we automatically use for example voice or gait to recognize known individuals on a day to day basis.

Not only facial recognition has been used throughout the history of civilization. Other biometrics have been used as a more formal means of recognition. For example, in southeastern France there is a cave, which is estimated to be at the very least 31 thousands years old, and its walls are adorned with paintings created by prehistoric men who lived there. Surrounding these paintings are numerous handprints that may have acted as an unforgeable signature of its originator [2].

It has been proved, that Babylonian business transactions are recorded in clay tablets that include fingerprints [3].

Joao de Barros, an European explorer and writer, claims that early Chinese merchants used fingerprints to settle business transactions. Some Chinese parents even used fingerprints to be able to tell their children from one another [4].

In the mid-1800's, a rapid growth of cities took place, mainly thanks to the industrial revolution and more productive farming. It became apparent that there is a need for the ability to formally recognize people. Various authorities and merchants were faced with increasingly larger and more mobile population. They could no longer rely solely on their own experiences and local knowledge. The courts of that era, influenced by Utilitarian thinkers, began to codify concepts of

justice that still exist to this very day. Most importantly, justice systems treated the first time offenders more leniently, and repeat offenders more harshly. This created a need for a formal system that recorded both offense(s) and measured identity traits of the offender. Even today, repeat offenders are treated more harshly than first time offenders. There were two different approaches.

The first one was the Bertillon system of measuring various body dimensions. This system is the invention of French ethnologist Alphonse Bertillon [4]. Bertillon took measurements of certain bony portions of the body, for example the skull width, foot length, cubit, trunk or left middle finger. These measurements, along with hair color, eye color and front and side view photographs, were recorded on cardboard forms. By dividing each of the measurements into small, medium and large groupings, Bertillon could place the dimensions of any single person into one of 243 distinct categories. Further subdivision by eye and hair color provided for 1,701 separate groupings. Standardization of the Bertillon System throughout the civilized world meant, that for the first time in recorded history, any individual (once classified), could be identified later. The benefit to police agencies was obviously incalculable. Although claims that emergence of this system would deplete the ranks of the professional criminals, were apparently too optimistic and premature.

The second approach was the formal use of fingerprints by police departements. By the late 1800's, a method was developed to index fingerprints. It provided the ability to retreive records just like Bertillon's system did, but it was based on a more individualized metric – fingerprint patterns and ridges. The first such robust system for indexing fingerprints was developed in India. This system was called the Henry System, because it was developed by Azizul Haque for police officer Edward Henry [4].

Automated biometric systems began to appear in the second half of the twentieth century, mainly due to the emergence of computer systems. The field of biometrics experienced a significant activity in the 1990's and began to appear in everyday applications in the early 2000's.

2.3 Biometrics today

Biometric technology has rapidly expanded into many areas of our society. We can see that biometric technologies are used in such diverse activities as entering amusement parks, accessing bank accounts and obtaining passports or driver's licenses. The use of biometrics has expanded steadily as the price of these high-tech devices has decreased significantly, and the complexity of integration and implementation has been greatly reduced. Biometric technology as a mean of protecting assets has been used for quite some time in some fields. For example intelligence, military, and law enforcement organizations have been using biometrics to enhance physical and logical access controls for decades. But in the past several years, there has been a significant increase in use of biometric technologies to protect valuable assets. For example, internet data centers often use biometric technologies for allowing personnel to access the data center floor or room. Fingerprint biometric devices are now present everywhere – built-in to laptops, PDAs or even USB drives. On some laptop models, facial recognition is available. Everyone who attended Superbowl XXXV had their faces compared with the faces of known criminals, using biometric technology. Walt Disney World in Orlando, Florida uses fingerprint readers to verify that customers who purchased multi-day passes are the same customers that re-enter the facility on subsequent days. Anyone entering the United States of America since September 30, 2004, has submitted prints of both index fingers. These are just a few examples demonstrating the increasing importance of biometrics in today's World.

2.4 Identity, identification and verification

Humans use some of the biometric characteristics to recognize known individuals on a day to day basis. Be it a voice, gait or face, our brain automatically recognizes known persons. This recognition

is based on an unique identity of an individual. Identity is a definite characteristic of an individual [1]. Although, this definition is for the physical identity, not an electronic identity, because anyone can create an unlimited number of electronic identities. Identity relates to another two terms – identification and verification.

Identification is 1:N, one-to-many recognition. It is the process of determining a person's identity by comparing a currently captured biometric template with all biometric templates present in the database. Identification systems are designed to determine identity based only on biometric information, no additional information, such as user ID or name, is provided. There are two types of identification systems: positive identification and negative identification.

Positive identification systems are designed to find a match for user's biometric information in a database of biometric information. Positive identification answers the *Who am I?* question, although the response does not have to be a name - it can be a user ID or some other unique identifier. A typical example of positive identification system is a prison release program where users do not enter a user ID or use a card, but simply look at a device that captures their iris and then they are identified.

Negative identification systems search databases in the same way, comparing one template against many, but these systems are designed to ensure that a person is not present in the database. This prevents people from enrolling twice in a system, and is often used in large-scale public benefits programs in which users may attempt to enroll multiple times in order to gain benefits under different names. Not all identification systems are based on determining a username or user ID. Some systems are designed to determine if a user is a member of a particular category. For example, an airport may have a database of known terrorists with no knowledge of their actual identities. System can return a match, but no knowledge of the person's identity is involved.

Verification is 1:1, one-to-one recognition. It is the process of establishing the validity of a claimed identity by comparing a currently captured biometric template with multiple biometric templates present in the database. Aside from a biometric trait, verification requires additional user information, for example name or user ID, then the individual's enrollment template is located and compared with the verification template. Verification answers the *Am I who I claim to be?* question. Some verification systems perform very limited searches against multiple enrollment records. For example, a user who had enrolled five fingerprint templates may be able to place any of the five fingers to verify, and the system performs 1:1 matches against the user's enrolled templates until a match is found. This is called 1:few (one-to-few) recognition. It is a middle ground between identification and verification. This type of application involves identification of a user from a very small enrollment database. While there is no definite threshold separating a 1:N from a 1:few system, any system that involves a search of more than 500 records is most likely classified as 1:N system. A typical example of 1:few system is access control to restricted areas at a small company (fifty or less employees), where users look at a iris capture device and are located from a small database.

2.5 Biometric system

Biometric system is essentially a system for pattern recognition [10]. It authenticates a person based on either physiological or behavioral biometric.

Physiological biometrics measure a specific part of the shape or structure of a portion of a subject's body. Physiological biometrics include facial scan, retina scan, hand scan, fingerprint and iris scan.

Behavioral biometrics are more concerned with how we do something, rather than just a static measurement of a specific body part. Behavioral biometrics include handwriting, keystroke dynamics, voice recognition and gait.

A generic biometric system consists of four main modules: a sensor module; a quality assessment and feature extraction module; a matching module; and a database module [10].

Sensor module: A suitable biometric scanner is required to acquire the raw biometric data of an individual. To obtain fingerprint images, for example, an optical fingerprint sensor may be used to image the friction ridge structure of the fingertip. The sensor module defines the human machine interface and is pivotal to the performance of the biometric system. A poorly designed interface can result in a high Failure to Acquire rate (FTA), resulting in a low user acceptability.
Since most biometric modalities are acquired as images (except for maybe voice which is audio based and odor which is chemical based), the quality of the raw data is also influenced by the characteristics of the camera technology that is used.

Quality assessment and feature extraction module: The quality of the biometric data acquired by the sensor is first assessed in order to determine its suitability for further processing. Usually, the acquired data is subjected to a signal enhancement algorithm in order to improve its quality. However, in some cases, the quality of the data may be so poor that the user is asked to present the biometric data again. The biometric data is then processed and a set of salient discriminatory features extracted to represent the underlying trait. During enrollment, this feature set is stored in the database and is commonly referred to as a template.

Matching and decision-making module: The extracted features are compared against the stored templates to generate match scores. The match score may be moderated by the quality of the presented biometric data. The matcher module also encapsulates a decision making module, in which the match scores are used to either validate a claimed identity or provide a ranking of the enrolled identities in order to identify an individual.

System database module: The database acts as the repository of biometric information. During the enrollment process, the feature set extracted from the raw biometric sample is stored in the database along with some personal information characterizing the user. The data captured during the enrollment process may or may not be supervised by a human depending on the application.

Biometric systems work through enrolling users by measuring and storing their particular biometric, and then later comparing the stored biometric data with data from unverified subjects to determine whether they should be allowed to access a system or location.

A biometric system's process has three main phases:

Enrollment - before a user can begin using a biometric system, he or she must complete an enrollment process. The objective of an enrollment process is to capture the particular biometric and store it in the database for later use. Usually the biometric system will request enrollment of several samples so that the system can determine an average and deviation. Depending on the biometric technology in use, there may have to be a faciliator to assist. The user may also has to provide other information such as name or user ID.

Usage - the biometric system will compare the sample with data stored in the database, and based on whether the biometric data matches or not makes a go or no go decision.

Update - for the type of biometrics that change over time, for example facial recognition or handwriting, a biometric system may need to update the data that was originally submitted at enrollment. This update may be performed either with each subsequent measurement or utilizing a separate update process.

Depending on the application context, a biometric system can operate either in verification or identification mode [10].

In **the verification mode**, the system validates a person’s identity by comparing the captured biometric data with her own biometric templates stored in the system database.

In such a system, an individual who desires to be recognized claims an identity, for example a user ID or user name, and the system performs a 1:1 recognition to determine whether the claim is true or not. Verification is typically used for positive recognition, where the main goal is to prevent multiple people from using the same identity.

In **the identification mode**, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system performs a 1:N recognition to establish an individual's identity without the subject having to claim an identity. The identification fails if the subject is not enrolled in the system database. Identification is a critical component in negative recognition applications where the system establishes whether the person is who she claims to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience - the user is not required to claim an identity. Traditional methods of personal recognition such as password, PIN, key, and token may work for positive recognition, but negative recognition can only be established through biometrics.

In general, a biometric system is easy to use, in most cases verification or identification takes only a few seconds. Even the enrollment process takes only a few moments. Using a biometric system is arguably faster than using an ID card or password, so this could be another positive fact for biometric systems.

2.6 Characteristics of a biometric system

Each biometric has its advantages and disadvantages, that results in the fact that the choice of a biometric trait for a particular application depends on a variety of variables and needs. Besides the matching performance, Jain et al. [10] have identified seven factors that determine the suitability of a physical or a behavioral trait to be used in a biometric application.

- **Universality:** Every individual using the application should posses the biometric trait.
- **Uniqueness:** The given trait must be sufficently different across the population.
- **Permanence:** The biometric trait of an individual should be stable over a period of time. A trait that significantly changes over a period of time is not a useful biometric.
- **Measurability:** It should be possible to acquire and store the biometric trait using devices that do not cause too much inconvenience to the individual. And the acquired data should be amenable to processing in order to extract representative feature sets.
- **Performance:** The recognition accuracy and the resources required to achieve that accuracy should meet the constraints imposed by the application.
- **Acceptability:** Individuals that will use the application should be willing to present their biometric trait to the system.
- **Circumvention:** This refers to the ease with which the trait of an individual can be imitated using artifacts (e.g., fake fingers), in the case of physical traits, and mimicry, in the case of behavioral traits.
- **Financial cost:** how much does the system cost, this can be a major factor [1].

Table 2.1 - Comparison of biometric technologies [11].

Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention
DNA	high	high	high	low	high	low	low
Ear	medium	medium	high	medium	medium	high	medium
Face	high	low	medium	high	low	high	high
Facial thermogram	high	high	low	high	medium	high	low
Fingerprint	medium	high	high	medium	high	medium	medium
Gait	medium	low	low	high	low	high	medium
Hand geometry	medium	medium	medium	high	medium	medium	medium
Hand vein	medium	medium	medium	medium	medium	medium	low
Iris	*high*	*high*	*high*	*medium*	*high*	*low*	*low*
Keystroke	low	low	low	medium	low	medium	medium
Odor	high	high	high	low	low	medium	low
Retina	high	high	medium	low	high	low	low
Signature	low	low	low	high	low	high	high
Voice	medium	low	low	medium	low	high	high

Table 2.1 shows comparison of biometric technologies. We can see that according to this table, the iris is one of the best biometrics overall.

2.7 Performance of a biometric system

Unlike password protected systems, where an exact match between two password strings is necessary in order to validate a user's identity, a biometric system rarely encounters two samples of a user's biometric trait that result in exactly the same feature set. This is caused by imperfect sensing conditions, changes in the user's biometric characteristic, changes in ambient conditions and variations in the user's interaction with the sensor. This means that two feature sets originating from the same biometric trait of a user rarely are exactly the same. Actually, it could be argued that a perfect match between two feature sets indicates the possibility that the system is under attack [10].

The variability observed in the biometric feature set of an individual is referred to as **intra-class variation**. The variability between feature sets originating from two different individuals is known as **inter-class variation**. A good biometric exhibits small intra-class variation and large inter-class variation [10].

The closeness of a match between two biometric feature sets is indicated by a score. A similarity match score is known as a **genuine** (authentic) score if it is a result of matching two

samples of the same biometric trait of a user. It is known as an **impostor** score if it involves comparing two biometric samples originating from different users [10].

An impostor score that exceeds the threshold η results in a false accept (**FAR**) or a false match (**FMR**), while a genuine score that falls below the threshold η results in a false reject(**FAR**) or a false non-match (**FNMR**) [10].

It should be mentioned, that FAR and FRR are not always treated as synonymous with FMR and FMNR, respectively [10]. The difference is that both FMR and FNMR also include FTM (*failure to match*) and FTA (*failure to acquire*) while FAR and FRR do not. Both FTM and FTA are discussed later in this chapter.

2.7.1 False Acceptance Rate - FAR

The *False Acceptance Rate* (FAR) is a measure of the likelihood that the access system will wrongly accept an access attempt; that is, will allow the access attempt from an unauthorized user. FAR is sometimes called **Type II Error rate** [10].

FAR can be defined as:

$$FAR = \frac{NFA}{NIIA}$$

or

$$FAR = \frac{NFA}{NIVA}$$

where:

FAR is the false acceptance rate
NFA is the number of false acceptance cases
NIIA is the number of impostor identification attempts
NIVA is the number of impostor verification attempts

2.7.2 False Rejection Rate - FRR

The *False Rejection Rate* (FRR) is one of the most important specifications in any biometric system. The FRR is defined as the percentage of identification instances in which false rejection occurs. It can be expressed as a probability [10].

FRR can be defined as:

$$FRR = \frac{NFR}{NEIA}$$

or

$$FRR = \frac{NFR}{NEVA}$$

where:

FRR is the false rejection rate
NFR is the number of false rejection cases
NEIA is the number of identification attempts
NEVA is the number of verification attempts

Except for these two types of errors mentioned above, a biometric system can encounter other types of errors as well, namely **Failure to Enroll** (FTE) and **Failure to Acquire** (FTA).

2.7.3 Failure to Enroll - FTE

The *Failure to Enroll* (FTE) rate denotes the proportion of users, that cannot be successfully enrolled in a biometric system. This means that user training may be necessary to ensure that an individual interacts with a biometric system correctly and that a good quality biometric data is acquired. This creates the need for robust and efficient user interfaces that can assist an individual both during enrollment and recognition [10].

FTE can be defined as:

$$FTE = \frac{NFE}{NNE}$$

where:

FTE is the failure to enroll rate
NFE is the number of unsuccessful enrollments
NNE is the number of all enrollments

2.7.4 Failure to Acquire - FTA

The *Failure to Acquire* (FTA) rate denotes the proportion of times the biometric device fails to capture a sample when the biometric characteristic is presented to it. This type of error typically occurs when the device is not able to locate a biometric signal of sufficiently good quality (e.g., an extremely faint fingerprint or an occluded face image). The FTA rate is also impacted by sensor wear and tear. This means that periodic sensor maintenance is instrumental for the efficient functioning of a biometric system [10].

FTA is defined as:

$$FTA = \frac{NEA}{NNA}$$

where:

FTA is the failure to acquire rate
NEA is the number of unsuccessful captures of biometric characteristic
NNA is the the number of all biometric characteristics presented to the system

2.7.5 Failure to Match – FTM

The Failure to Match (FTM) – the number of biometric characteristics that the system is not able to match against its database [10].

FTM can be defined as:

$$FTM = \frac{NFM}{NNM}$$

where:

FTM is the failure to match
NFM is the number of all rejected matches
NNM is the number of all attempts to match

2.7.6 Equal Error Rate – EER

The Equal Error Rate (EER) is the point where False Acceptance Rate equals False Rejection Rate. A lower EER value therefore indicates better performance. The EER is the best single description of the Error Rate of an algorithm and is often used for quick comparison of two biometric systems [10].
The perfect biometric system has EER equal to 0, that means that the FAR and FRR curves do not touch, so far such a system does not exist and most likely never will.

3 Iris recognition technology

The idea of using the iris as a distinguishing human identifier was first suggested in 1885 by Alphonse Bertillon [4]. He described both color and pattern type. British ophthalmologist James Doggart commented specifically on the complexity of iris patterns and suggested that they might be sufficiently unique to serve in the same way as fingerprints in 1949 [10].

Today, iris recognition is generally viewed as one of the most reliable and accurate biometric system available. It has been deployed in large-scale systems that have been very effective. Majority of commercial iris recognition systems use patented algorithms developed by Dr. Daugman [10], and they are able to produce perfect recognition rates. Although the fact that the published results have usually been produced under favourable conditions must be considered.

3.1 The human iris

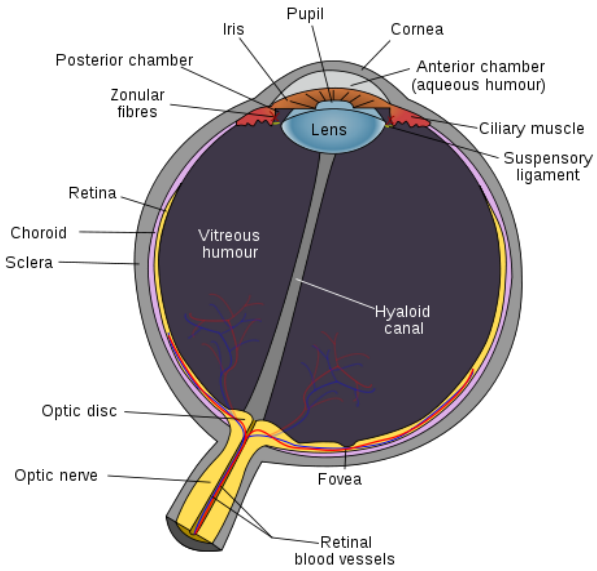


Figure 3.1 – The human eye, iris is located between the cornea and the lens.

The iris is the pigmented muscular curtain near the front of the eye, between the cornea and the lens, that is perforated by an opening called the pupil. The iris is located in front of the lens and ciliary body and behind the cornea. It is bathed in front and behind by a fluid known as the aqueous humour. The iris consists of two sheets of smooth muscle with contrary actions: dilation (expansion) and contraction (constriction). These muscles control the size of the pupil and thus determine how much light reaches the sensory tissue of the retina. The sphincter muscle of the iris is a circular muscle that constricts the pupil in bright light, whereas the dilator muscle of the iris expands the opening when it contracts [9].

The human iris begins to form during the third month of gestation and the structure is complete by the eighth month of gestation, although pigmentation continues into the first year after birth. The iris grows from the ciliary body and its colour is given by the amount of pigment and by the density of the iris tissue. The most important function of the iris is controlling the size of the pupil. The amount of light reaching the pupil and falling on the retina of the eye, is controlled by muscles in the iris. They regulate the size of the pupil and determine the amount of light entering the

pupil. The change in the size results from involuntary reflexes is not under conscious control. The tissue of the iris is soft and loosely woven and it is called the stroma of iris.

Figure 3.2: The human iris with pupil in the middle, the iris patterns are clearly visible.

Figure 3.2 clearly shows the iris patterns. The iris patterns are complex and consist of a large variety of features including collagenous fibers, crypts, color, rifts and coronas. The iris pattern is set prior to birth where the iris muscle goes through folding and then degeneration. After the first to second year after birth, it varies little except due to eye diseases. Since the patterns are so stable and unique, iris is a very good biometric.

3.2 Iris as a biometric

Using iris as a biometric has both advantages and disadvantages.

Advantages:

- Iris is a highly protected, internal organ of the eye.
- Iris is visible from a distance.
- Iris patterns possess a high degree of randomness.
- Changing the size of the pupil confirms natural physiology.
- Limited genetic penetrance.
- Iris is stable throughout life.

Disadvantages:

- Iris is a small target (approximately 1cm) to acquire from a distance (approximately 1m).
- Iris is a moving target.
- Iris must be located behind a curved, wet and reflecting surface.
- Iris is obstructed by eyelashes, eyelids and reflections.
- Iris deformations are non-elastic as the pupil changes size.

A *good biometric* must have [12]:

- **Large inter-class variability** – large differences between individuals
- **Small intra-class variability** – small differences between samples taken from a particular individual
- **Stability over time** – related to small intra-class variability
- Relative **ease of collection**

Iris has a large inter-class variability. The detailed structure and distribution of the stroma fibers comes about from processes during gestation that have sensitive dependence on initial conditions. The processes are similar to tearing a sheet of paper. Two sheets taken in succession from

a ream of paper and subjected to a careful attempt to tear them in exactly the same way will tear differently. Experiments have shown that the details of the iris are at least as distinct as fingerprints in automated biometric identification systems [12]. Biometric templates from the most widely used algorithm have approximately 250 degrees of freedom [10] in the context of a binomial model for the imposter distribution. Iris patterns have small intra-class variability and appear stable over time.

Usually, iris cameras are set to capture an image of the iris in the near infrared range, because at this wavelength the iris structure is most apparent. Varying quality of eye images must be considered. Good quality image is shown in *Figure 3.3*, iris pattern is clearly visible and there are no obstacles in the image.

On the other hand, we must also consider that there are several potential problems. For example **contact lens**. Nowadays, many people wear contact lenses on a day to day basis. Contact lenses come in many forms, and not all of them are optically clear. All contact lenses sit in front of the iris, so they will distort, to some degree, the visible filaments. If an individual enrolls with a contact lens and then verifies without one, it may cause some difficulties.

Another thing that should be considered is the **eye rotation**. If the eye is not looking directly at the camera when the image is being taken it may rotate about an axis. This may cause some of the filaments in the eye to be distorted.

Occlusion may occur and a part or the whole iris may be occluded by either the eye lid blinking, the person squinting or glasses getting in the way. *Figure 3.4* shows an occlusion - the eye is partially closed.

Dilation is another problem. Pupil dilation occurs when the iris muscle contracts, and it causes the iris filaments to be compressed. Pupil dilation can occur due to lighting extremes, arousal or drugs. *Figure 3.5* shows a highly dilated pupil.

Environment may be a major factor. The environment lightning may cause over or under exposure of the image, making distinguishing the iris filaments difficult.

Eyelashes present another obstacle, long eyelashes can obscure part of the iris, causing sections of the iris to be unreadable.

Certain **medical conditions** can cause problems by distorting the iris.

Glasses may affect the optical properties of reading through the lens, especially if the lens is tinted or has a gradient power. Glasses may also collect dust and scratches, both of which can obscure parts of the iris.

Glare from lighting or environment reflection can obscure part of the iris.

There is a lot of different **iris variants**. For example, some racial subgroups have very dark eyes, which leads to iris structure not being visible well.

Although a minor inconvenience, **height** can also be a factor. Some iris recognition cameras are fixed in certain height, and for example people in a wheelchair may not be able to get in the right position.

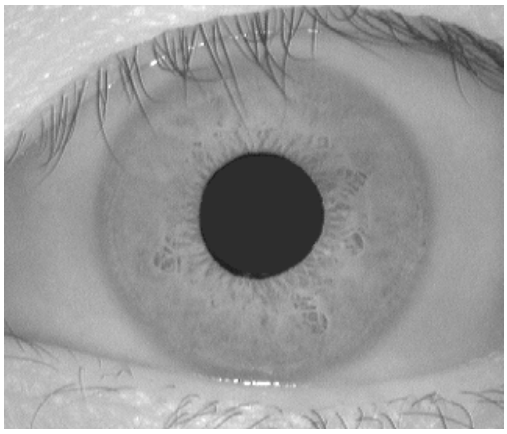


Figure 3.3 – Good quality - fibrous structure is clearly visible

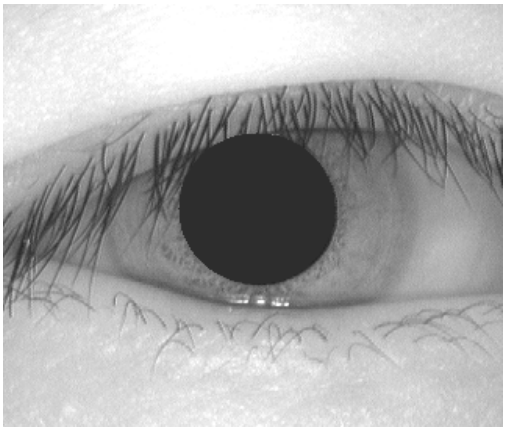


Figure 3.4 – Occlusion - partially closed eye obscures part of the iris

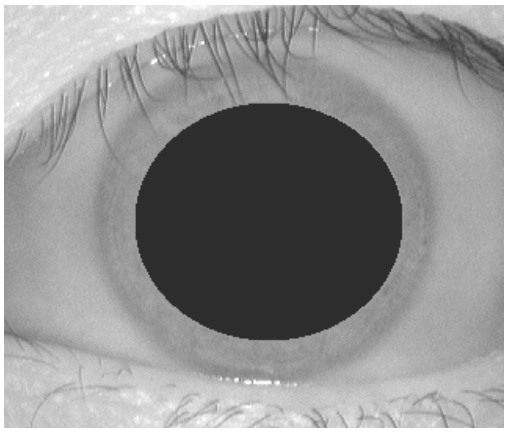


Figure 3.5 – Dilatation - filaments are distorted and compressed to edge

4 Iris recognition devices and software

My original objective was to get familiar with the OKI IrisPass-M iris recognition camera, study it and afterwards evaluate the whole system – perform tests of both verification and identification. Unfortunately, I found out that the OKI IrisPass-M in conjunction with the BioAPI v1.1 framework can not return the closeness of a match between two irides and there is no way to set the threshold for accepting the two irides as a match. The system only returns a negative result (return value is 0), that is if verification or identification was not successful; or a positive result (return value is 1790) if verification or identification was successful. This restriction exists to guarantee that the False Acceptance Rate (FAR) is 1 in 1.2 million, but on the other hand it prevents any kind of extensive testing and research.

After discussing this unfortunate fact with my supervisor, Ing. Petr Dittrich, I decided to abandon the idea of performing extensive tests on OKI IrisPass-M and the BioAPI framework. Instead, I decided to focus on eye iris recognition technology in general. This gave me a chance to briefly study and test two more iris recognition devices – the Panasonic Authenticam BM-ET100US and the Iribio iris mouse. These two devices, along with the OKI IrisPass-M are discussed later in this chapter.

Except for the BioAPI v1.1 framework, I also got a chance to study two more iris recognition software products. The first system is the VeriEye 2.2 iris recognition algorithm, developed by Neurotechnology [6]. The second system is an open source iris recognition software developed by Libor Masek [7]. This open source iris recognition system proved to be the most suitable software for testing and research, because it is easy to modify. Masek's iris recognition system is completely written in MATLAB, which is an interpreted language, so his iris recognition system is slow. Therefore, I decided to optimize the original code by implementing computationally intensive parts in C, adding a graphical user interface, as well as adding the option to save eye images to a database and modifying the code so the system displays the closeness of a match for each pair of irides that are being compared. Operating threshold determining whether the two irides match or not can be easily set by editing one particular variable. For lack of better term, this system will be referred to as the Iris Recognition System in MATLAB from now on. All three iris recognition software products are discussed in this chapter as well.

4.1 OKI IrisPass-M

Figure 4.1 - OKI-IrisPass-M

OKI IrisPass-M is a fully automatic iris recognition camera developed by OKI Electric Industry Co., Ltd., it features an intuitive user interface, rapid throughput, voice guidance and compilance with international standards. [5]

This device is extremly easy to use. The process of capturing is completly non-touch operation. All that is needed for capturing the iris is to take a position 30-60cm from the device and follow the voice instructions, a green light will appear and the biometric template is stored or compared with others. The whole process does not take more than a few seconds.

OKI IrisPass-M Specification [5]:

Image Capture speed	1 second or less (speed may vary depending on conditions)
Iris Identification speed	1 second or less (at proper PC configuration)
False Acceptance Rate	1 in 1.2 million
Operational range	30 – 60cm user's height: 145-200cm
Size	328(weight) x 197(height) x 84(depth) mm
Weight	5 kg
Power supply	AC100-240V, 50-60Hz
Operating environment	Temperature: 0-40°C Humidity: 30-80%
Networking	100base-T, LAN
Software	BioAPI™ v1.1 PrivateID® v2.3

The particular model I worked with has serious overheating problem. It would not work for more than 30 or 40 consecutive minutes, and a cool down was required every time this problem occurred. This significantly slowed down the performance testing, and was also part of the reason why I decided to focus on iris recognition technology in general and carried out only basic tests on the OKI IrisPass-M.

Overall, OKI IrisPass-M is still the best iris recognition device I had a chance to work with, and despite the overheating problems, which may or may not be unique to this particular model, it is still a very quick and easy to use iris recognition camera. Although for extensive testing and research a suitable software would have to be developed. The BioAPI framework v.1.1 that came with the camera is suited for end user application, rather than testing and research, since there is no way to set the operating threshold.

4.2 Other iris recognition devices

I had a chance to briefly study and test the Panasonic Authenticam BM ET100 and the Iribio iris mouse. Both of these devices are portable and neither is meant to be used as a high security system. The *Panasonic Authenticam BM ET100* behaved as a web camera, not iris recognition system. PrivateID software was installed, but neither me or my supervisor, Ing. Dittrich, were able to use this device for enrollment or even capturing the iris. No tests involving this device were carried out. The *Iribio iris mouse* is clearly meant to be used as an additional layer of security for personal computers. It came with software that allows for securing files, directories or even the whole system. For accessing assets protected by this system, a verification is required. Although the system failed to enroll and verify on numerous occasions, in the end I was able to successfully enroll and then verify both of my irides. No further tests were carried out on this device. Neither of these devices is suited for iris recognition tests, although they can be useful for protecting personal assets.

4.3 Iris recognition software

Overall, I tested three different iris recognition software products. BioAPI Framework 1.1 was tested in conjunction with the OKI IrisPass-M, while the other two software products – VeriEye 2.2 and Iris Recognition System in MATLAB were tested using unique eye images, since neither of these two products support OKI IrisPass-M device.

BioAPI Framework v1.1 is a proprietary software, an outdated version – version 1.1 (version 2.0 is the latest) was available with the OKI IrisPass-M device. My plan was to add an identification functionality to an already existing sample application, but this plan was deemed meaningless after I found out that this software in conjunction with the OKI IrisPass-M device does not support manual setting of the operating threshold.

The **VeriEye 2.2** iris recognition algorithm is also a proprietary software, developed by Neurotechnology. It is recognized by NIST as one of the most accurate and reliable iris recognition algorithms available. This software features robust eye iris detection, automatic interlacing detection and correction, correct iris segmentation, fast matching and reliability [6]. On the other hand, it is quite expensive – standard SDK costs 790EUR, extended version costs 1290EUR, and so far only 3 iris scanners and platforms (Cross Match I Scan 2, Vista FA2 / VistaFA2E iris camera and VistaMT Multimodal Biometric Device) are supported.

The Iris Recognition System in MATAB is discussed in a more detail below.

4.3.1 Iris Recognition System in MATLAB

The **Iris Recognition System in MATLAB** is built on a software that was developed by Libor Masek [7]. He made part of his software available for testing and research purposes. That gave me a chance to study an iris recognition system in a greater detail. Masek's code was easy to modify, which allowed me to optimize and modify the code so that the program is suitable for iris recognition technology testing and research. This system is composed of several sub-systems, corresponding with each state of iris recognition. Firstly, the iris region in the eye image must be located – this process is generally called segmentation. Next, a dimensionally consistent representation of the iris must be created – this is called normalization. And finally, feature encoding – a template containing the most discriminating features of the iris are created. The input to the system is a grayscale eye image, and the output is an iris template, which is a mathematical representation of the iris region.

The segmentation is a very important stage of iris recognition, because the data that is falsely interpreted will result in corrupted templates, and will lead to poor recognition rates. The success of segmentation heavily depends on the image quality of the eye images. Fortunately, eye images that were used for testing do not contain any specular reflections.

After successful segmentation, the next step is to transform the iris region so that it has fixed dimensions, which allows for comparisons. The dimensional inconsistencies between eye images are caused mainly by the stretching of the iris, which is caused by pupil dilation from varying levels of illumination. Other sources of inconsistency are varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket. The normalization process produces iris regions, which have the same constant dimensions, so that two images of the same iris under different conditions have characteristic features at the same spatial location.

The most discriminating information present in an iris pattern must be extracted in order to provide accurate iris recognition of individuals. Only the significant features of the iris must be encoded so that comparisons between templates can be made. The template generated in the feature encoding process will also need a corresponding matching metric, which gives a measure of similarity between two iris templates. This metric should give one range of values when performing intra-class comparisons, and another range of values when performing inter-class comparisons.

Confirming this assumption is one of the objectives of testing. The difference between intra-class and inter-class comparisons should be enough to decide whether the two irides match. In comparing two bit patterns, the Hamming distance is the count of bits different in the two patterns [8]. The Hamming distance is used as a metric for recognition, because bit-wise comparisons were necessary.

5 Tests and results

In this chapter, performed tests are described and achieved results are discussed. Tests were performed on OKI IrisPass-M, VeriEye 2.2 software and finally Iris Recognition Software in MATLAB.

5.1 OKI IrisPass-M - tests

Basic recognition tests were performed on 21 individuals, 20 male students aged 19-21, and one 21 years old female student. Everyone was told what to do in order to successfully enroll both irides. Enrollment went fine for all participants, although in one instance, the process had to be repeated. Next, verification tests were performed, each participant attempted to verify three times, that means 63 verifications were performed overall. Verification was successful for all participants, and there were no false rejections.

$$FTE = \frac{1}{22} = 4{,}5\%$$

$$FRR = \frac{0}{63} = 0\%$$

$$FAR = \frac{0}{63} = 0\%$$

OKI IrisPass-M had no problems with classic contact lenses, out of the 21 participants, four wear contact lenses, including myself. I successfully enrolled while wearing contact lenses and then successfully verified without contact lenses. This also worked vice versa. This was surprising finding for me, since the border of the contact lens is slightly visible so I thought that it would confuse the system in detecting it as the iris boundary.

On the other hand, participants wearing standard optical glasses were not able to successfully enroll and verify while wearing the glasses. They had to be taken off in order to sucessfully enroll and verify. This fact could be considered a minor inconvenience.

5.2 CASIA eye image database

To test the VeriEye 2.2 software and the Iris Recognition System in MATLAB I decided to use the Chinese Academy of Sciences - Institute of Automation (CASIA) eye image database.
This database was obtained by sending an application form to the Chinese Academy of Sciences - Institute of Automation. CASIA eye image database version 1 was used for all tests. It contains 108 unique eyes (classes), and there are 7 images of each unique eye, in total there is 756 eye images. Images from each class were taken in two sessions with one month interval between them. The images were captured especially for iris recognition research using specialised digital optics developed by the National Laboratory of Pattern Recognition, China. Thanks to specialized imaging conditions using near infra-red light, features in the iris region are highly visible and there is good

contrast between pupil, iris and sclera regions. These characteristics make this database an ideal testing material. The eye images in this database are from persons of Asian decent, whose eyes are characterised by irises that are densely pigmented, and with dark eyelashes.

5.3 Iris Recognition System in MATLAB

CASIA eye image database was used to test this iris recognition system. Out of the 108 unique eyes, 35 randomly selected unique eyes were added to the program database. Each unique eye represents one class, and each class consists of 7 eye images. The eye images were taken in two sessions with one month interval between them. This is a crucial information, since one of the objectives is to prove the stability and uniqueness of the iris. So, in total, 245 eye images were enrolled.

5.3.1 System performance

First, the performance of this system was evaluated. The goal was to determine False Acceptance and False Rejection rates for various thresholds. I decided to test the system with seven different operating thresholds. Hamming distance values *0,2*; *0,25*; *0,3*; *0,35*; *0,4*; *0,45* and *0,5* were chosen. The two lowest and highest values were not expected to produce good results, but they were necessary to create FAR and FRR graphs.

For test purposes, each enrolled eye image was compared with all the other eye images present in the database. For detailed results see Appendix A. Because each class contains seven eye images, 49 positive matches are expected for each class, and there are 35 classes in total. That means that the overall expected number of positive matches is 49 times 35, which equals 1715. Overall, 245 times 245 (60025) comparisons were made. This iris recognition system never failed to recognize two exact images as equal and in this case always returned Hamming distance equal to zero. In most cases only two exact eye images produced score lower than 0,2, the only exceptions were classes 3 and 28 (see Appendix A), these two had very small intra-class variability.

As expected, threshold set to 0,2 proved to be too low, since system with this setting accepted only 261 irides, although 1715 irides should have been accepted. System never falsely accepted an iris. That means that the False Acceptance Rate is 0%, but on the other hand, False Rejection rate is as high as 84,781%. Such False Rejection rate is obviously unacceptable, even for a very high security systems.

Threshold set to 0,25 also proved to be too low, system with threshold set to 0,25 accepted only 517 irides, despite the fact that 1715 irides should have been accepted overall. Once again, system never falsely accepted an iris. Therefore, False Acceptance Rate is still 0%, but False Rejection Rate is still too high – 69,854%.

Threshold set to 0,3 also turned out to be too low, but there had been a significant improvement compared to the two lower thresholds. 1119 out of 1715 irides were accepted, False Acceptance Rate is once again 0%, since there were no false acceptances, and False Rejection Rate went down to 34,752%, still rather high number, but this is the first threshold setting that could be even considered to be used as an operating threshold, and could be potentially chosen for a very high security systems, where security has much higher priority than user convenience.

A system with threshold set to 0,35 accepted 1508 out of 1715 irides, once again, no false acceptances occurred, so False Acceptance Rate is still 0% and False Rejection Rate went down again. This time to 12,069%, which could be acceptable for high security systems.

Threshold set to 0,4 turned out to be the best threshold setting. The system accepted 1649 out of 1715 irides, and for the last time, system never falsely accepted an iris, therefore, False Acceptance

Rate is still 0%, and False Rejection Rate is only 3,848%. This is by far the best FAR/FRR ratio achieved in these tests. This operating threshold would be the best choice for common systems, since it still provides 0% False Acceptance rate, and False Reject is only 3,8%, which is only a minor inconvenience for the users.

With threshold set to 0,45, for the first time, system falsely accepted an iris. Out of 60025 comparisons, 7039 irides were accepted by the system, although only 1715 irides should have been accepted. That means that for the first time, False Acceptance rate is as high as 11,726%, and False Rejection Rate is 0%, since no iris was falsely rejected. This setting would be unacceptable for any kind of system.

As expectd, a system with threshold set to 0,5 would be utterly useless. Out of 60025 comparisons, system accepted 59861 irides, although only 1715 irides should have been accepted. No false rejections occured, therefore, False Rejection Rate is 0%, but False Acceptance Rate is a whopping 99,726%.

Threshold	0,2	0,25	0,3	0,35	0,4	0,45	0,5
Irides accepted	261	517	1119	1508	1649	7039	59861
Expected result	1715	1715	1715	1715	1715	1715	1715
Difference	1454	1198	596	207	66	5324	58101
Comparisons total	60025	60025	60025	60025	60025	60025	60025
FAR	0,00%	0,00%	0,00%	0,00%	*0,00%*	11,73%	99,73%
FRR	84,78%	69,85%	34,75%	12,07%	*3,85%*	0,00%	0,00%

Table 5.1 – Overall results, see Appendix A for more details

Table 5.2 sums up the test results, we can clearly see, that threshold set to 0,4 produced the best results, the system has not falsely accepted any user and falsely rejected only 66 out of 1715 irides. We must also consider, that the segmentation process is imperfect and is the most likely cause of some of these false rejections. If a carefully selected sub-set of the CASIA eye image database was used instead, the results would most likely be even better, but this test was not intended to be carried out under perfect conditions. See **Appendix A** for detailed tests records.

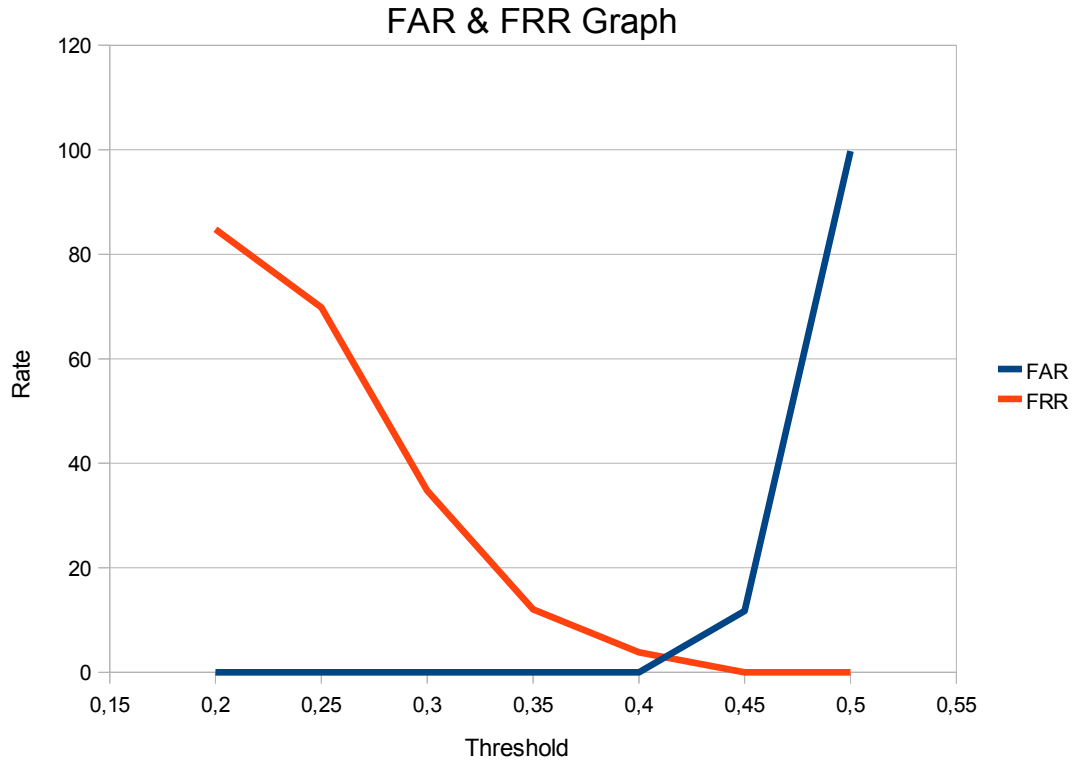


Figure 5.1 – FAR & FRR graph, sometimes called Equal Error graph. It shows the False Accept and False Reject rates at all thresholds.

Figure 5.1 shows False Acceptance Rate and False Rejection Rate at all thresholds. Minimising the crossover (Equal Error Rate) is generally the goal of a researcher. Information on how well is the system handling Impostors can be seen from the steepness of the FAR plot. This graph is often used to determine the operating threshold, and we can see that threshold set to 0,4 is the best choice, since False Acceptance rate is 0% and False Rejection Rate is only 3,85%.

A closer look at the crossover (Equal Error Rate) is shown in **Figure 5.2** (below).

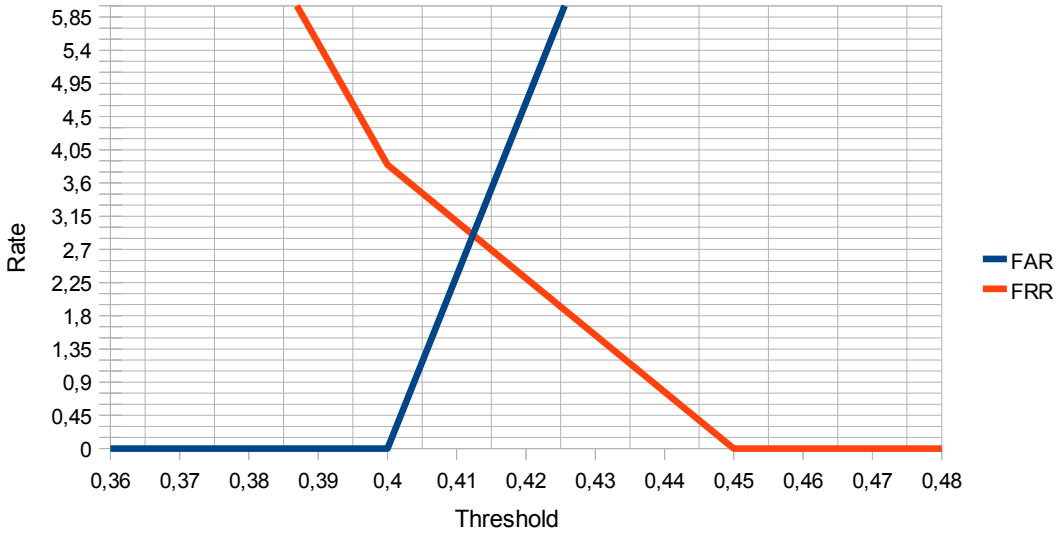


Figure 5.2 – A closer look at the crossover - Equal Error Rate.

In *Figure 5.2* we can see that the point of intersection (EER) of the two curves occurs at coordinates [0,4125;0,2875].

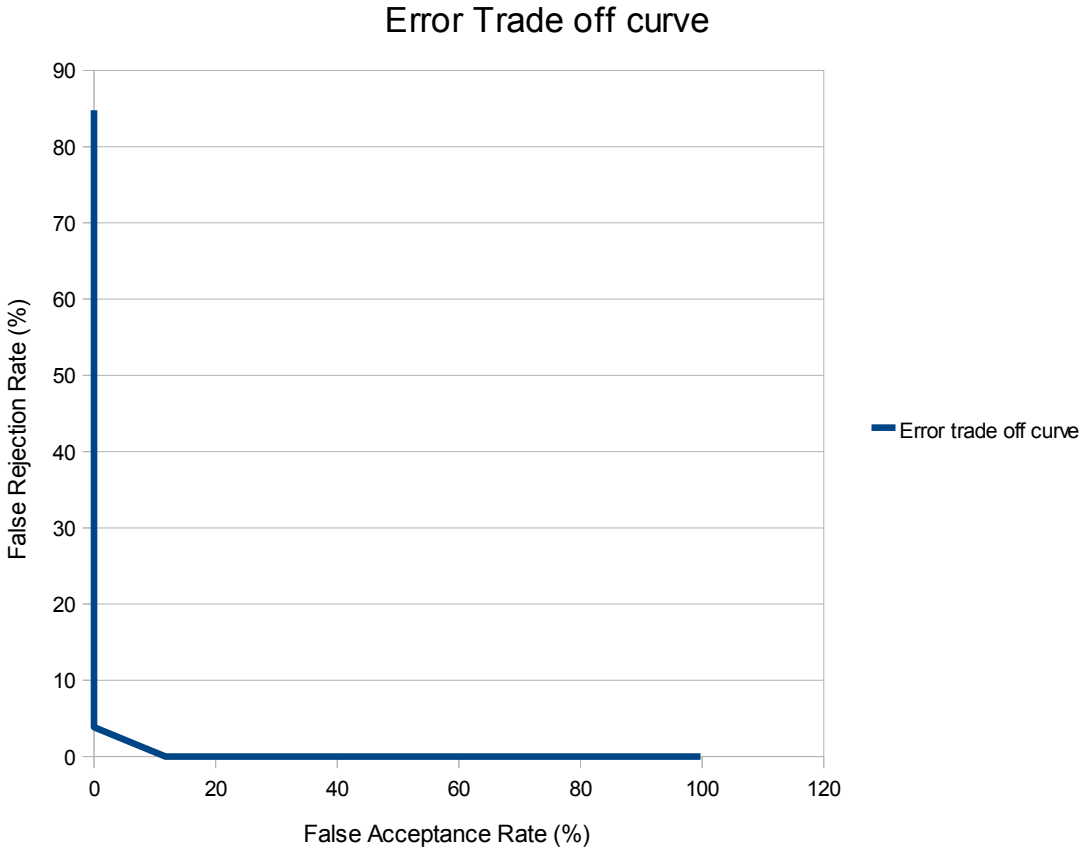


Figure 5.3 – Error Trade off curve

Figure 5.3 shows the Error Trade off curve, this plot is very useful for displaying the trade-off between False Accept and False Reject rates. The closer the plot lies to the axis, the better the performance of the biometric system. We can see that the tested iris recognition system performed very well, the trade-off for 0% False Acceptance Rate is approximately 4% False Rejection Rate.

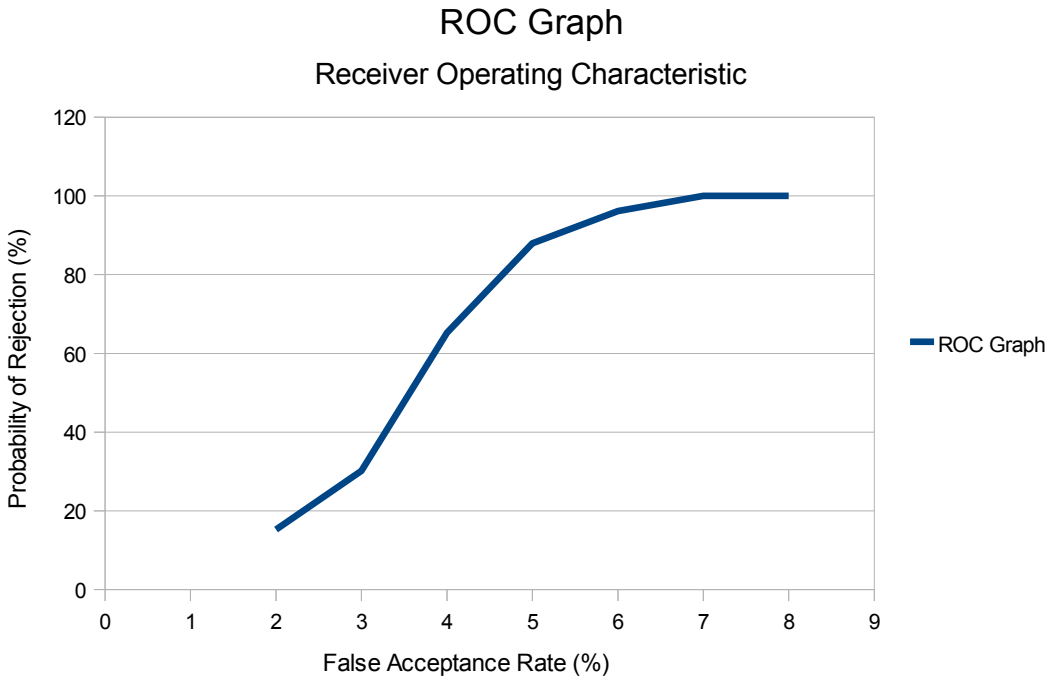


Figure 5.4 – Receiver Operating Characteristic

Figure 5.4 shows the Receiver Operating Characteristic (ROC). The ROC is one the most widely quoted graphs for biometric systems. This graph displays the Probability of rejection against the False Acceptance rate. The Probability of rejection, sometimes called Genuine Accept Rate, equals to 1 minus FRR, that is why this graph is very similar to the Error trade off curve.

5.3.2 Uniqueness of iris patterns

Test was performed to confirm uniqueness of iris patterns, it is important, because iris recognition relies on iris patterns from different eyes being independent. Uniqueness of iris patterns was determined by comparing templates generated from two different eyes with each other. Produced Hamming distance values were then examined. Then the results were compared with Hamming distance values produced by comparing templates created from eye images of one individual.

According to statistical theory, the mean Hamming distance for inter-class comparisons should be 0.5. That is because the bits in each template can be considered to be randomly set, that means there is a fifty percent chance of a bit being set to one and a fifty percent chance of a bit being set to zero. This means that between two templates, half of the bits will agree and half will disagree, resulting in a Hamming distance of 0.5.

Another goal is to confirm that there is a distinct difference between intra-class and inter-class comparisons. Twenty randomly selected unique eyes from CASIA eye image database were used (140 eye images in total). The achieved results are shown in the tables below.

Intra-class comparisons:

Class ID	Mean Hamming distance value (including the same image-to-image comparison)	Mean Hamming distance value (excluding the same image-to-image comparison)
1	0,221515	0,258434
2	0,241577	0,281840
3	0,180618	0,210721
4	0,263568	0,307496
5	0,275957	0,321950
6	0,182163	0,212524
7	0,324005	0,378006
8	0,307943	0,359267
9	0,272660	0,318103
10	0,280276	0,326989
11	0,273206	0,318740
12	0,270373	0,315435
13	0,263568	0,307496
14	0,276631	0,322736
15	0,298494	0,348243
16	0,259697	0,302980
17	0,255242	0,297783
18	0,227666	0,265610
19	0,218846	0,255321
20	0,244365	0,285092

Table 5.2 – Shows mean Hamming distance value for intra-class comparisons

We can see, that there is a difference between the two columns. In the first column, there are mean Hamming distance values for intra-class comparisons, with all 7 images compared to each other, that means 49 comparisons were made within one class. On the other hand, the second column contains mean Hamming distance values for intra-class comparisons, but the same images were not compaerd to each other, that means that only 42 comparisons were made within one class. This was done in order to determine how big of a difference the same image-to-image comparison makes, since this iris recognition system returns 0 as a Hamming distance value when two same images are compared.

If the same image-to-image comparisons were included, the mean Hamming distance value was **0,256919**, and the number went up to **0,299738** if those comparisons were not included. That means, that on average, the difference between these two comparisons is **0,042819**, which is not a significant difference, but it is worth mentioning.

Inter-class comparisons:

Class ID	Mean Hamming distance value
1	0,469566
2	0,467629
3	0,470323
4	0,470662
5	0,470325
6	0,336378
7	0,324005
8	0,466841
9	0,472831
10	0,426523
11	0,469908
12	0,383923
13	0,470662
14	0,466232
15	0,466681
16	0,468719
17	0,468987
18	0,470856
19	0,472343
20	0,469417

Table 5.3 – Shows mean Hamming distance value for inter-class comparisons

For the inter-class comparison the mean Hamming distance value is **0,456332**, which confirms that the iris patterns are indeed independent. The difference between mean Hamming distance values produced by intra-class and inter-class comparisons is **0,199413**, this proves that there is, as expected, a distinct difference between intra-class and inter-class comparisons, which is one of the characteristics of a good biometric.

5.4 VeriEye 2.2

Using CASIA eye image database, basic tests were performed to confirm the claimed performance. The whole CASIA eye image database was enrolled and identification tests were carried out. Achieved results depended on program settings, ideal threshold proved to be FAR set in interval < 0.1; 0.00001>, this resulted in no false rejections or false acceptances. FAR greater than 0.1 resulted

in several cases of false acceptance, while the False Rejection Rate was still 0%. On the other hand, when FAR was less than 0.000001, as expected, False Rejection Rate went up.

Overall, this software performs very well, is very fast and supports various settings, the only disadvantages are that this software supports only a handful of iris recognition devices and is quite expensive.

5.5 Tests - conclusion

OKI IrisPass-M proved to be a reliable, fast and easy to use iris recognition camera. Despite some technical problems, it performed well with 0% False Acceptance Rate and 0% False Rejection Rate. Although the sample was small (only 21 people), it is still a perfect score. Unfortunately, at the moment there is no software that would work with the device and at the same time allowed for setting the operating threshold. BioAPI v1.1 framework is more suited for end-user application rather than research.

VeriEye 2.2 algorithm performed according to its settings, and the proclaimed performance has been confirmed. This system is very fast, the only downside is that not very many iris recognition cameras are supported, so tests had to be carried out using the CASIA eye image database.

Iris Recognition System in MATLAB turned out to be the only software that can be modified at will, and with the operating threshold set to correct value, it produced good results. In order to find the best operating threshold, performance tests were carried out. 35 randomly selected classes (each class contains 7 eye images) from CASIA eye image database were used. This system was also helpful in the process of confirming uniqueness of iris patterns and proving that there is a distinct difference between intra-class and inter-class comparions. On the other hand, despite implementing computationally intensive parts in C, the Iris Recognition system in MATLAB is still slower than for example VeriEye 2.2. At the moment, this system does not support any iris recognition cameras. If it was decided to further develop this systém, in order to support some iris recognition cameras, current system speed would most likely become an issue and whole system would have to be implemented in C or C++.

6 Conclusion

Biometric technologies are becoming more and more popular, they provide safe and convenient alternative to classic ID cards or passwords. The iris recognition technology is generally considered to be one of the most reliable biometric technologies available today. This thesis is devoted to evaluation of the technology. Firstly, basic biometric principles and terms were described, and some of the features of the human iris were mentioned. Next, this thesis describes the devices and software that underwent the testing. Finally, test results are discussed.

The main objective was to evaluate iris recognition technology, and although OKI IrisPass-M was not the centerpiece of testing in the end, an alternative has been found, an open-source iris recognition system was heavily modified in order to evaluate iris recognition technology. The performed tests can be divided into two categories – performance tests and tests confirming the uniqueness of the iris.

The goal of performance tests was to find the best operating threshold in order to minimize False Acceptance and False Rejection rates. Tests were successful and a threshold with sufficiently good False Acceptance Rate / False Rejection Rate ratio has been found.

The tests performed in order to confirm uniqueness of the iris were also successful, it has been proved that there is indeed a distinct difference between intra-class and inter-class comparisons of the irides, which is one of the necessary characteristics of a good biometric. Furthermore, the mean Hamming distance value for inter-class comparisons proved to be high enough to confirm that the iris patterns are indeed independent.

It has been proven that the human iris is a good biometric, and that the iris recognition is accurate and reliable biometric technology.

Although the Iris Recognition System in MATLAB turned out to be sufficiently accurate, there is a lot of room for improvement. First of all, the system is still quite slow, although it is much faster than the original version, for real-time iris recognition, the speed would not be sufficient and the whole system would have to be implemented in C or C++. A more convenient functionality for adding eye images to the database could be realized. Another issue is imperfect segmentation, a more elaborate algorithm for detecting eyelids and eyelashes could be implemented in order to produce the best results. Support for iris recognition cameras, such as OKI-IrisPass-M, could be added as well, although if this was to happen, at the very least the speed and segmentation issues would have to be addressed.

Working on this thesis gave me a chance to study basic principles biometrics – an area that had been completely unknown to me before, I encountered some interesting technologies and thoroughly enjoyed testing of the iris recognition technology. In the future I would like to add more features to the Iris Recognition System in MATLAB and perform large-scale tests on real iris recognition camera using this system.

Bibliography

[1] DRAHANSKÝ, M.: *Biometrické systémy – studijní opora*. [online], 2006-01, [cit.5-5-2010]. Dostupné z WWW: <https://www.fit.vutbr.cz/study/courses/BIO/private/BIO_Studijni_opora.pdf>

[2] RENAGHAN, J.: *Etched in Stone*. [online], 1997-07, [cit.5-5-2010]. Dostupné z WWW: <http://nationalzoo.si.edu/publications/zoogoer/1997/4/etchedinstone.cfm>

[3] ASH, B.: *Problems With Fingerprint Biometrics*. [online], 2010-2, [cit.6-5-2010]. Dostupné z WWW: <http://ezinearticles.com/?Problems-With-Fingerprint-Biometrics&id=3783105>

[4] OSBORNE, A.: *Biometrics history*. [online], 2005-8, [cit.6-5-2010]. Dostupné z WWW: http://www.video-surveillance-guide.com/biometrics-history.htm

[5] Oki.com [online]. 2005 [cit. 2010-05-13]. *Oki IRISPASS®-M*. Dostupné z WWW: <http://www.oki.com/en/press/2005/z05049e-2.html>.

[6] Neurotechnology.com [online]. 2010 [cit. 2010-05-13]. *VeriEye SDK*. Dostupné z WWW: <http://www.neurotechnology.com/verieye.html>.

[7] MASEK, Libor. Csse.uwa.edu.au [online]. 2003 [cit. 2010-05-13]. *Source Code*. Dostupné z WWW: <http://www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html>.

[8] Planetmath.org [online]. 2007 [cit. 2010-05-13]. *Hamming Distance*. Dostupné z WWW: <http://planetmath.org/encyclopedia/HammingDistance.html>.

[9] *Iris* : Encyclopædia Britannica Article. In Iris. Chicago : Encyclopædia Britannica, 2010. s. 1.

[10] JAIN, A, et al. *Handbook of Biometrics*. Springer, 2008, ISBN 978-0-387-71040-2.

[11] MALTONI, D. *Handbook of Fingerprint Recognition*. Springer, 2003, ISBN 0-387-95431-7.

[12] TISTARELLI, Massimo, et al. *Handbook of Remote Biometrics*. Springer, 2009, ISBN 978-1-84882-384-6.

Appendix A

Experimental results

ID refers to class ID
T refers to threshold

ID	T = 0,2	T = 0,25	T= 0,3	T = 0,35	T = 0,4	T = 0,45	T = 0,5
1	7	25	45	49	49	158	1713
2	7	7	13	27	39	253	1713
3	21	47	49	49	49	196	1711
4	7	11	25	37	37	238	1705
5	7	7	17	39	49	168	1709
6	7	9	33	45	49	196	1703
7	7	9	23	39	49	270	1710
8	7	11	31	47	49	123	1715
9	7	7	25	47	49	175	1706
10	7	9	19	41	49	276	1709
11	7	9	21	29	37	243	1710
12	7	7	27	47	49	208	1709
13	7	7	31	45	49	193	1714
14	7	23	42	49	49	162	1710
15	7	9	21	43	49	241	1713
16	7	11	39	47	49	206	1714
17	7	25	49	49	49	131	1708
18	7	7	21	45	49	174	1693
19	7	9	17	25	31	222	1713
20	7	17	41	47	49	222	1711
21	7	9	21	37	49	104	1713
22	7	9	41	49	49	200	1706
23	7	7	43	49	49	240	1715
24	7	21	37	47	49	165	1715
25	7	11	39	49	49	170	1714
26	7	11	29	47	49	232	1709

27	7	13	29	37	47	122	1709
28	9	29	47	49	49	159	1714
29	7	38	49	49	49	286	1711
30	7	7	11	15	37	236	1705
31	7	11	19	47	49	233	1714
32	7	17	45	47	49	225	1710
33	7	29	46	48	49	164	1712
34	7	29	49	49	49	298	1713
35	7	10	25	43	49	150	1712

Appendix B

CD contents

The **src** directory contains source codes for the Iris Recognition System in MATLAB.

The **CASIA** directory contains 756 grayscale eye images that can be used for testing.

Appendix C

Iris Recognition System in MATLAB – usage and requirements

To use this program, Matlab Image Processing Toolbox is required. This program was successfully tested using MATLAB 7.9.0.529 (R2009b). 32-bit Windows OS is required as well.

The program is very easy to use. All source files (*iris.m*, *mex.c* and *readme.m*) must be copied to current MATLAB directory, the program can then be run by typing **iris** in the main MATLAB window.

Once is the program running, there are several options available. Firstly, an image can be selected and added to the database or identification can be performed. For verification, two images must be selected. For more information read program help available via program menu.