

FACULDADE DE ENGENHARIA DA UNIVERSIDADE DO PORTO



Liveness Detection in Biometrics

Ana Rute Caetano Louro

Mestrado Integrado em Engenharia Eletrotécnica e de Computadores

Supervisor: Prof. Jaime Cardoso

Co-Supervisor: Ana Filipa Sequeira

July 31, 2014

A Dissertação intitulada

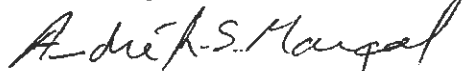
“Liveness Detection in Biometrics”

foi aprovada em provas realizadas em 23-07-2014

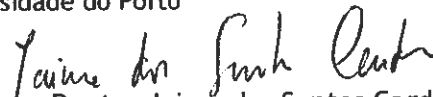
o júri



Presidente Professor Doutor Ricardo Santos Morla
Professor Auxiliar do Departamento de Engenharia Eletrotécnica e de Computadores
da Faculdade de Engenharia da Universidade do Porto



Professor Doutor André Ribeiro da Silva Marçal
Professor Auxiliar do Departamento de Matemática da Faculdade de Ciências da
Universidade do Porto



Professor Doutor Jaime dos Santos Cardoso
Professor Auxiliar do Departamento de Engenharia Eletrotécnica e de Computadores
da Faculdade de Engenharia da Universidade do Porto

O autor declara que a presente dissertação (ou relatório de projeto) é da sua exclusiva autoria e foi escrita sem qualquer apoio externo não explicitamente autorizado. Os resultados, ideias, parágrafos, ou outros extratos tomados de ou inspirados em trabalhos de outros autores, e demais referências bibliográficas usadas, são corretamente citados.



Autor - Ana Rute Caetano Louro

Faculdade de Engenharia da Universidade do Porto

Resumo

Sistemas biométricos de reconhecimento são mais vantajosos em relação aos métodos de reconhecimento usuais pois permitem que um indivíduo seja reconhecido por aquilo que é e não pelo que sabe ou tem em sua posse.

Dois dos traços biométricos usados atualmente neste tipo de sistemas são a íris e a impressão digital. Estes traços têm características únicas que permitem a distinção e o reconhecimento de pessoas, no entanto, podem ser reproduzidos ou usados de forma fraudulenta.

Um possível modo de defraudar um sistema de reconhecimento automático é através da apresentação de uma reprodução falsa do traço biométrico usado ao sensor. Uma forma de tentar subverter o número de casos de admissão de utilizadores falsos que tentam aceder ao sistema da forma acima descrita é através do estudo da vivacidade do traço biométrico apresentado ao sensor. Assim, no âmbito desta dissertação, serão estudados e testados algoritmos de deteção de vivacidade da íris e da impressão digital.

No caso da íris, o estudo foca-se em casos em que lentes de contacto são utilizadas para tentar defraudar o sistema de reconhecimento. Quanto à impressão digital, bases de dados com exemplares falsos obtidos a partir de moldes de impressões digitais reais são utilizadas para testar os métodos escolhidos.

Os algoritmos utilizados são replicações de algoritmos do estado da arte, os quais são testados para os dois traços biométricos escolhidos, tendo como objectivo estudar não só a precisão de cada algoritmo individualmente, mas também comparar a sua performance em cada traço biométrico.

Os resultados mostram que é possível obter resultados semelhantes ou até melhores que os obtidos no estado da arte, usando outras bases de dados de iris e impressões digitais, mas isso não acontece para todas as bases de dados testadas, provando, então, que ainda é necessário melhorar ou talvez combinar os algoritmos, de modo a reduzir ainda mais a taxa de erro de classificação.

Abstract

Biometric recognition systems are more advantageous than traditional methods of recognition as they allow the recognition of an individual for what he is and not for what he possesses or knows. Two of the currently most used biometric traits are the iris and the fingerprint. These traits have unique characteristics that allow people's recognition and distinction. However, they can also be reproduced or used fraudulently.

A possible way of accessing the system fraudulently is by presenting a fake reproduction of the biometric trait to the sensor. A way of preventing that could be by assessing the liveness of the biometric trait. Therefore, in the context of this dissertation, liveness detection algorithms for iris and fingerprint will be studied and tested.

Concerning this, for the iris images the study is focused on cases where contact lenses are used to spoof the recognition system. For the fingerprint, databases with fake samples obtained from molds of real fingerprints are used to test the methods.

The replicated algorithms are state of the art methods that were tested in both biometric traits, iris and fingerprint. Their accuracy is individually studied and their performance are also compared when the method is used with iris images and fingerprint images, aiming to assess if the same approach can be used in both cases.

The results show that it is possible to obtain results comparable or even better than the state-of-the-art ones, using other iris and fingerprint databases, but that does not occur for every database tested. This proves that it is still necessary to improve or maybe combine the algorithms, so that the classification error rate drops.

Agradecimentos

Começo por agradecer ao meu orientador, Professor Jaime Cardoso, pela oportunidade de realizar este projecto em colaboração com o VCMI, pela orientação global do trabalho e propostas de soluções nos momentos em que os obstáculos me atingiram em força.

Agradeço igualmente à minha co-orientadora, Ana Filipa Sequeira, sem a qual esta dissertação não teria tido pernas para andar. Um muito sincero obrigada por toda a sua paciência, dedicação, disponibilidade e apoio fornecidos durante estes últimos seis meses de desenvolvimento desta dissertação.

Uma palavra de apreço aos restantes membros do VCMI pelo apoio prestado, pelas questões, sugestões, explicações e simpatia.

Agradeço ao João e ao Zé, por me acompanharem sempre nas pausas para café ou almoço, mesmo que algumas delas fossem apenas uma desculpa para libertar um pouco a mente do trabalho, e por me darem sugestões, dicas e apoio quanto a este processo, pelo qual também já passaram.

Estou também grata a todos os amigos que fiz nestes últimos seis anos, sem os quais o meu percurso académico não teria sido nem 1/10 tão divertido quanto o foi. As memórias das serenatas, das aulas às 8h da manhã, das tardes na AE e por aí fora, tornaram tudo tão especial...

Um gigante abraço também, às minhas amigas Rey, Tatiana, Marta, Cláudia e Inês, por me apoiarem neste capítulo que agora termina, por se mostrarem sempre interessadas na minha dissertação e no rumo que esta levava ao longo do semestre e por perceberem a minha ausência em certas ocasiões.

Por último, mas com certeza mais importante, agradeço, do fundo do meu coração, à minha família, especialmente aos meus pais, que nunca deixaram de me apoiar e que acreditaram sempre no meu sucesso, mesmo quando eu própria não acreditava.

Ana Rute Louro

"I love those who can smile in trouble, who can gather strength from distress, and grow brave by reflection. 'Tis the business of little minds to shrink, but they whose heart is firm, and whose conscience approves their conduct, will pursue their principles unto death."

Leonardo da Vinci

Contents

1	Introduction	1
1.1	Context	1
1.2	Overview	1
1.3	Motivation	2
1.4	Objectives	2
1.5	Structure	3
2	Biometrics' Overview	5
2.1	Historical Context	5
2.2	Definition	5
2.3	Biometric Traits	6
2.4	Biometric Systems	7
2.4.1	Architecture	7
2.4.2	Operating Mode	8
2.4.3	Accuracy Measurements	8
2.5	Spoofing Attacks & Countermeasures	9
2.5.1	Accuracy Measurements	11
3	State of the Art	13
3.1	Iris Recognition and Liveness Detection	13
3.1.1	Eye Anatomy	13
3.1.2	Iris Databases	14
3.1.3	Iris Recognition Methods	18
3.1.4	Commercially Available Solutions	22
3.1.5	Iris Liveness Detection	24
3.2	Fingerprint Recognition and Liveness Detection	29
3.2.1	Fingerprint Anatomy	29
3.2.2	Fingerprint Databases	30
3.2.3	Fingerprint Recognition Methods	31
3.2.4	Fingerprint Sensors	33
3.2.5	Fingerprint Liveness Detection	39
3.3	Summary	43
4	Methodology	45
4.1	Segmentation	45
4.2	Algorithms	46
4.2.1	Algorithm I - Weighted Local Binary Patterns	46
4.2.2	Algorithm II - Gray Level Co-occurrence Matrices	49

4.3	Classification	53
5	Experimental Setup and Results	55
5.1	Databases	55
5.1.1	Iris	55
5.1.2	Fingerprint	55
5.2	Feature Extraction	55
5.2.1	Weighted Local Binary Patterns	55
5.2.2	Gray-Level Co-Occurrence Matrices	56
5.3	Learning methodology	56
5.3.1	Feature Selection	56
5.3.2	Classification results using SVM	56
5.3.3	Cross-Validation	57
5.4	Evaluation Metrics	57
5.5	Results for the Iris images	57
5.6	Results for the Fingerprint images	59
5.7	Feature Selection Test	61
5.8	Comparative analysis with State of the Art	62
5.8.1	Comparison of methods' results in different databases	62
5.8.2	Comparison of different methods' results using the Notre Dame, Clarkson and LivDet2013 databases	63
6	Conclusions and Future Work	67
6.1	Conclusions	67
6.2	Future Work	68
7	Appendix	69
7.1	Iris Results Graphs - Comparative analysis with State of the Art	69
7.2	Fingerprint Results Graphs - Comparative analysis with State of the Art	70
7.3	Feature Selection Test	73
	References	75

List of Figures

2.1	Classification of Biometric Traits	7
2.2	Scheme of a typical Biometric System	8
2.3	Representation of FAR and FRR	9
2.4	Vulnerable points of Biometric Systems	10
3.1	Human Eye Anatomy	13
3.2	Photograph of a Human Eye	14
3.3	Examples of iris images from BATH database	14
3.4	Examples of iris images from CASIA database	15
3.5	Examples of iris images from ICE database.	15
3.6	Examples of iris images from WVU database	16
3.7	Examples of iris images from UBIRIS.v1 database	16
3.8	Examples of iris images from UBIRIS.v2 database	16
3.9	Examples of iris images from MMU database	17
3.10	Examples of iris images from UPOL database	17
3.11	Examples of iris images from MobBIO database	18
3.12	Schematic diagram of Daugman's iris recognition method	19
3.13	Normalization of the iris image through Daugman's Rubber Sheet	20
3.14	Schematic diagram of Wildes' iris recognition method	21
3.15	Use of printed iris images in a biometric system	24
3.16	Examples of cosmetic contact lenses	25
3.17	Examples of iris images from CLARKSON database	27
3.18	Examples of iris images from NOTRE DAME database.	27
3.19	Examples of iris images from WARSAW database.	28
3.20	Examples of iris images from MobBIOfake database	28
3.21	Examples of iris images from BIOSEC database	29
3.22	The main fingerprint pattern types.	29
3.23	Core and delta points; Fingerprint minutiae details	30
3.24	Examples of fingerprint images from FVC2006 database	31
3.25	Fingerprint recognition system block diagram	31
3.26	A fingerprint image faded into the corresponding direction map	32
3.27	Fingerprint image and corresponding binarized skeleton	32
3.28	Typical structure of a fingerprint scanner	34
3.29	Example of fingerprint scanners	34
3.30	Examples of plain, rolled, swept and multiple fingerprints.	35
3.31	FTIR fingerprint acquisition	35
3.32	Optical-fibers fingerprint acquisition	36
3.33	Electro-optical fingerprint acquisition	37

3.34	Capacitive fingerprint acquisition	38
3.35	Ultrasound fingerprint acquisition	39
3.36	Finger model and mold	40
3.37	Examples of live fingerprints from the LivDet2013 datasets	42
3.38	Examples of fake fingerprints from the LivDet2013 datasets	42
3.39	Examples of live and fake fingerprints from the ATVS database	43
4.1	Reference points obtained with the manual segmentation	46
4.2	Representation of the Gaussian scale space generation	47
4.3	Gradient orientations & Histogram of orientations	47
4.4	Local Binary Pattern method scheme	48
4.5	Weighted LBP process	48
4.6	Weighted LBP at different scales	49
4.7	GLCM method - Iris image pre-processing	50
4.8	Example of the creation of a GLCM matrix	50
4.9	Directions used for the GLCM calculations	53
5.1	Classification Errors for the wLBP method	62
5.2	Classification Errors for the GLCM method	63
5.3	Classification Errors for the Notre Dame database	64
5.4	Classification Errors for the Clarkson database.	64
5.5	Biometrika Classification Errors	65
5.6	CrossMatch Classification Errors	65
5.7	Italdata Classification Errors	65
5.8	Swipe Classification Errors	65
7.1	Classification Errors for the Notre Dame database	69
7.2	Classification Errors for the Clarkson database	70
7.3	Biometrika Classification Errors	70
7.4	CrossMatch Classification Errors	71
7.5	Italdata Classification Errors	71
7.6	Swipe Classification Errors	72

List of Tables

2.1	Comparative analysis of Biometric Traits	7
3.1	Advantages and disadvantages of Wildes' method	22
5.1	Results of the SVM Classifier for GLCM and weighted LBP Features using Iris images	58
5.2	Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - Biometrika dataset	59
5.3	Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - CrossMatch dataset	59
5.4	Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - Italdataset dataset	60
5.5	Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - Swipe dataset	60
5.6	Best results for the each type of fake mold	61
5.7	Features selection results for the Crossmatch dataset with the GLCM method . .	61
7.1	Feature Selection mean error results for the CrossMatch dataset	73

Symbols and Abbreviations

3D	Three dimensional
2D	Two dimensional
ATM	Automated teller machine
BATH	University of Bath Iris Image Database
BSIF	Binarized Statistical Image Features
CASIA	Institute of Automation Chinese Academy of Sciences Iris Image Database
CMOS	Complementary metal–oxide–semiconductor
CCD	Charge-coupled Device
DB	Database
EER	Equal Error Rate
FAR	False Accept Rate
FFT	Fast Fourier Transform
FRR	False Rejection Rate
FTIR	Frustrated Total Internal Reflection
FVC	First Verification Competition
GLCM	Gray Level Co-occurrence Matrices
ICE	Iris Challenge Evaluation Iris Image Database
ID	Identification
IR	Infra-red
IRIS	Iris Recognition Immigration System
LBP	Local Binary Pattern
LED	light-emitting diode
LPQ	Local Phase Quantization
MatLab	Matrix Laboratory
MMU	Multimedia University Iris Image Database
NIST	National Institute of Standards and Technology
RFID	Radio-Frequency Identification
RGB	Red Green and Blue additive color model
ROI	Region of Interest
SIFT	Scale Invariant Feature Transform
SVM	Support Vector Machine
UBIRIS	University of Beira Interior Iris Image Database
UID	Unique Identification
UPOL	Univerzita Palackého V Olomouci Iris Image Database
VCMi	Visual Computing and Machine Intelligence
WLB	Weber Local Descriptor
wLBP	Weighted Local Binary Pattern
WVU	West Virginia University Iris Image Database

Chapter 1

Introduction

1.1 Context

This work was developed in the context of the Curricular Unit (EEC0020) - Dissertation, from the Integrated Master in Electrical and Computer Engineering from the Faculty of Engineering of Porto University. It was done in collaboration with the VCMI (Virtual Computing and Machine Intelligence) group at INESC TEC - Porto.

In order to provide global information about this project and update the state of it, a website was created and is available at <http://paginas.fe.up.pt/~ee08206>.

1.2 Overview

Personal recognition is the process of determining the identity of a particular individual from a database of known people [1]. Recognizing someone's identity has been a concern of modern societies now that the restriction of access to data is crucial in almost every contemporary field, mostly due to fraud attempts and other illegal attacks. The most frequent recognition applications are the ones used for criminal investigation, access to security systems or restricted areas, border control and access to computers or cellphones.

The traditional way of validating one's identity is by using something that can be *possessed* or *learnt*, as a magnetic card, Radio-Frequency Identification (RFID) card or a password. However, as items and keys can be lost, stolen, forgotten or revealed, enabling fraudulent usage, it is known that a more reliable way of recognition is by using something that *one is*, instead of something that *one has* or *knows*.

For this reason, the application of biometrics in recognition systems is becoming conventional. This phenomenon is arising due to the fact that biometrics recognition systems operate based on physical or behavioral features, called biometric traits, which are usually exclusive of each person [1].

A biometric recognition system can use one or several human traits as samples, being the most commonly adopted the fingerprint, the speech, the face, the iris or the retina.

The fingerprint is the most known biometric trait used in recognition systems and it is still the most used one due to its easiness of acquisition, high distinctiveness, persistence, and acceptance by the users [2].

On the other hand, iris recognition is increasingly employed in admission systems and it is constantly evolving. It has been considered as one of the strongest recognition methods due to the characteristics of the human iris, which are usually exclusive to a singular individual.

The fact that the iris is such an exclusive human feature becomes a huge advantage when used in recognition systems. However, contrary to what was believed to be true, recent researches [3, 4] conclude that the aging of an iris template is possible and it leads to the increment of the error rate between an enrollment image and an image taken for the recognition process, a few years after.

1.3 Motivation

Currently, iris and fingerprint recognition systems can be found worldwide with outstanding rates of success.

Whilst recognition methods evolve, new ways of spoofing them break out as well, creating a need for safer solutions in order to guarantee the authenticity of the collected images.

Prior to the recognition process, especially in a scenario where no human control is required, the system should be able to recognize whether a biometric trait is real or if someone is trying to access the system fraudulently. One way of achieving that is by assessing the liveness of the sample.

Since both iris and fingerprints are rich in texture, the same methods of detecting the liveness of the traits could be, theoretically, applied to them. The challenge now is to test if a method performs the same way with different traits or if the characteristics of iris and fingerprints influence the accuracy of a liveness detection method.

1.4 Objectives

The aim of the dissertation “Liveness Detection in Biometrics” is to review existing algorithms for liveness detection in iris and fingerprint recognition systems.

These two biometric traits were chosen because one of them is the most known trait (fingerprint) and the other has been gaining popularity in this type of system (iris). Also, they are both known for their advantages in terms of unique anatomical characteristics.

One of the objectives of this work is to test iris liveness detection algorithms in cases where cosmetic contact lenses are used, as this is a relatively new way of spoofing recognition systems.

Two databases containing patterned contact lenses were used to test the selected algorithms, which are *Notre Dame* and *Clarkson*.

The second stage of this project is to test the same algorithms in fingerprint databases with fake samples. The database chosen for this trait was the *LivDet2013*.

With the results from both tests, we should be able to compare the effectiveness of the used methods in two different biometric traits.

1.5 Structure

The remaining chapters of this document are organized as follows: Chapter 2 gives a brief overview of the global topic of this dissertation, “Biometrics”. Chapter 3 describes the State of the Art of the topics related to the proposed work. This Chapter is sub-divided in: Iris Recognition and Liveness Detection and Fingerprint Recognition and Liveness Detection. A brief summary is presented as the last topic in this chapter.

Chapter 4 presents the methodology and algorithms used during the development of this dissertation, followed by Chapter 5 where the practical setup and results are presented and analyzed.

Lastly, Chapter 6 gives the conclusions, difficulties found and future work suggestions for this theme.

Chapter 2

Biometrics' Overview

2.1 Historical Context

It is known that the first biometric scientific system for human identification appeared in the 19th century. However, the use of biometrics as a way of identifying people has been present in the human life since prehistorical times, as palm prints were found in ancient petroglyphs and it has been said that those handprints were used to sign the paintings [5].

Also, around 200 BC, Chinese records include descriptions of the use of handprints as evidence during robbery investigations, revealing that the first applications of biometrics as we know it were mainly for forensic and law enforcement use. It is known that, later, also in China, palms and feet of children were stamped on paper to register them [6].

As quoted in the first paragraph, the first science-based identification system appeared in the 19th century, created by Alphonse Bertillon, who introduced the use of a number of anthropomorphic measurements to identify criminals. Due to the fact that Bertillon's system was time consuming and, not much later on, the use of fingerprints became the standard security biometric system worldwide, his system quickly became obsolete [7].

Lately, modern societies are becoming concerned about the security and accuracy of recognition systems due to the increase of terrorist acts and scam schemes. There is, then, a need to exploit other biometric features, which may be more impervious to attacks than fingerprints.

Nowadays, several systems are using other types of characteristics, such as face, iris, or speech and those systems are applied not only for forensic purposes, but also to a range of other things like accessing a room or a computer, or authenticating in a public network.

2.2 Definition

The etymology of the word "biometrics" comes from the Greek "bio-" which refers to one's life, course or way of living, and "-metros" which means measure [8]. Even though this term has been previously used in the field of statistics to refer to the analysis of biological data (which is now known as biostatistics), it is generally used to refer to an automated method of authenticating

individuals based on anatomical or behavioral human characteristics [9, 10].

The fact that biometrics use physical or observable characteristics makes it a reliable solution to authenticate individuals since it recognizes unique features that are not secret, i.e. even though everyone can see the physical/behavioral characteristics of the subject, they cannot memorize them in order to access the authentication system [10].

The use of a specific anatomic trait relies upon its *distinctiveness* and *permanence*. The accuracy of the system depends, ultimately, on those two premises and how much they hold true for general population [7].

The use of biometrics can be split in two branches: *identification* and *verification*. Identification implies establishing a person's identity based on his/hers biometric traits and aims to answer the question: "*Who is this person?*". Verification, on the other hand, involves confirming or denying someone's identity, aiming to reply the query: "*Is this person who he/she claims he/she is?*" [9].

2.3 Biometric Traits

Biometric traits are physical and behavioral human features used by identification and verification applications. The most common human features used for biometric purposes are:

- Fingerprint;
- Iris;
- Face;
- Voice;
- Signature;
- Hand Geometry;
- DNA;
- Keystroke;
- Gait.

Physical traits normally refer to a part of the human body like the face, the eyes, the hands, etc. On the other hand, behavioral traits relate to the conduct of a person, e.g. the voice or the signature. Biometric traits can also be labeled as genotypic or phenotypic. Genotypic features are genetically defined, while phenotypic features can be changed over time and depend on the surrounding environment [11, 12].

Figure 2.1 illustrates the division of those traits in the correspondent categories of physical or behavioral.

The choice of a trait for a biometric system can affect the effectiveness and efficiency of it, so there are some aspects that biometric traits are expected to have and that should be taken into account while developing a recognition system:

- **Universality** - Every person must possess their specific variation of the trait;

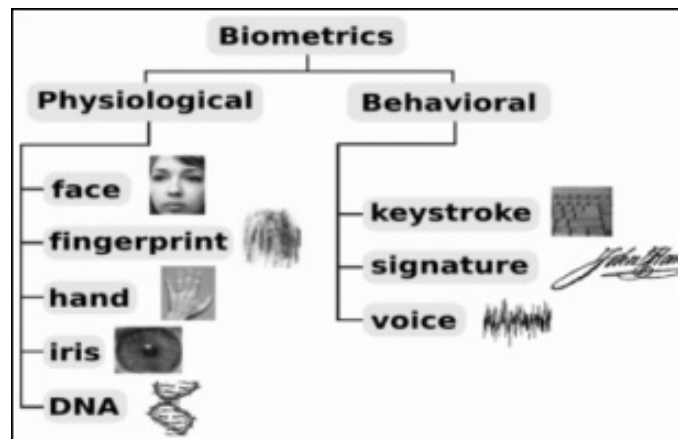


Figure 2.1: Classification of Biometric Traits [12].

- **Uniqueness** - No one should share the same specific variation of the trait;
- **Permanence** - The trait should not be changeable or alterable;
- **Collectability** - The trait should be readily presentable to a sensor and easily quantifiable.

In Table 2.1 a comparison between the aforementioned biometric traits is illustrated:

	Universality	Uniqueness	Collectability	Permanence
Fingerprint	Medium	High	Medium	High
Iris	High	High	Medium	High
Face	High	Low	High	Medium
Voice	Medium	Low	Medium	Low
Signature	Low	Low	High	Low
Hand Geometry	Medium	Medium	High	Medium
DNA	High	High	Low	High
Keystroke	Low	Low	Medium	Low

Table 2.1: Comparative analysis of Biometric Traits. Adapted from [13].

2.4 Biometric Systems

2.4.1 Architecture

A biometric system can be divided in two stages: the enrollment and the identification/verification. The enrollment consists in acquiring data from specific individuals so that a database can be built. It can be said that the enrollment is the registration of individuals to the database and those will be the ones who should be recognized during the identification or verification process.

The second stage of a biometric system is the identification which, no matter what feature is chosen to work with, follows the process schematized in Figure 2.2. It can be split in five modules.

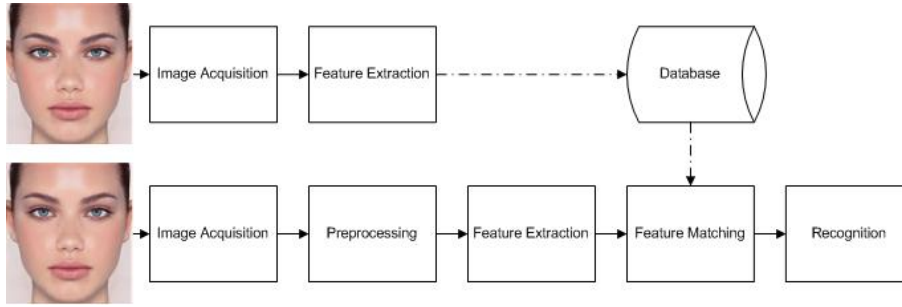


Figure 2.2: Scheme of a typical Biometric System. Adapted from [11, 13].

The process starts with the capture of the images, acquiring a biometric sample, followed by a preprocessing module where several steps can be taken like segmentation, normalization and liveness detection. The third part of the process consists in the feature extraction, where conspicuous features are identified for classification. Lastly, the features are compared and matched with stored ones, resulting in a possible recognition [13, 14].

2.4.2 Operating Mode

As referred in Section 2.2, biometrics can be used for both identification and verification.

The verification system aims to confirm or deny a person's identity by comparing his/her biometric template with the stored ones, evaluating the probability of this person being who he/she claims to be. For this purpose a 1:1 matching algorithm is used .

In an identification mode, the individual's biometric feature is compared to the entire database, which means that a 1:N matching algorithm is used. The objective of this process is to detect the person's ID. The success of both these operating modes depends on the presupposition that the person using the system has already been through the enrolment process. In addition, there are several ways of spoofing these systems, but this topic will be discussed hereafter [9, 13].

2.4.3 Accuracy Measurements

Even though it is not possible to give a single value that reflects the accuracy of a recognition system, there are some measures of accuracy that can be used under the same data and following the same protocol that can be helpful when trying to evaluate the effectiveness of a biometric system.

One way of comparing one system to another, both using the same biometric trait, is by analyzing its False Acceptance Rate (FAR) [11]. The FAR is the proportion between the number of False Acceptances (FA), i.e. the number of impostors that were able to enter the system, and the total number of impostors that try to access the system: the falsely accepted and the truly rejected (TR):

$$FAR = \frac{FA}{FA + TR} \quad (2.1)$$

The FAR measures, then, the probability of confusing two identities, but it is only meaningful when presented simultaneously with the False Rejection Rate (FRR).

The FRR is the probability of the identity of a valid user being denied and it can be calculated as the proportion between the False Rejections (FR) and the total number of users that try to access the system, the falsely rejected and the truly accepted (TA).

$$FRR = \frac{FR}{FR + TA} \quad (2.2)$$

Figure 2.3 shows a graphical representation of FAR and FRR values for distinct similarity threshold values. The point where the two lines intersect represents the Equal Error Rate (EER) and is a very common measure of the biometric systems accuracy. It gives the average error rate when the FAR and FRR are approximately the same.

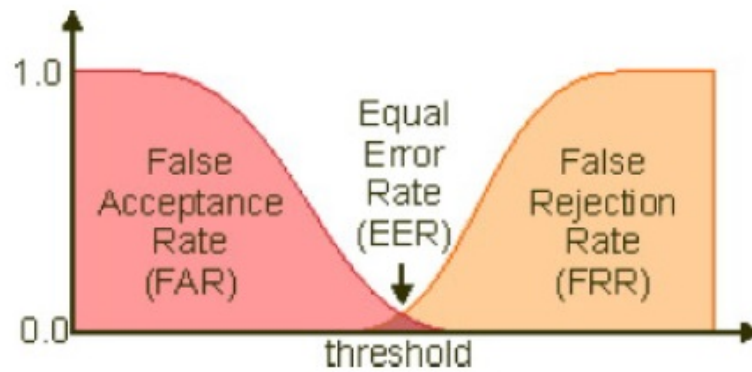


Figure 2.3: Representation of FAR and FRR [13].

2.5 Spoofing Attacks & Countermeasures

Biometric systems are known to be robust and trustworthy, nevertheless, there are ways of spoofing them. In Figure 2.4, eight points of vulnerability of biometric recognition systems are presented. Spoofing attacks can be divided in two groups: *direct attacks* and *indirect attacks* [15].

It is called a *direct attack* when a fake sample is presented to the sensor, which corresponds to point number one in Figure 2.4. Examples of direct attacks would be the copy of a signature, the usage of a face mask or the usage of a printed picture.

Indirect attacks use some additional knowledge of the system and access its components. In Figure 2.4, points 2 to 8 correspond to indirect attacks:

- *Point 2* - In this attack mode, an old stored biometric signal is resubmitted into the system, disregarding the sensor. This type of attacks can also be called a “replay” attack;

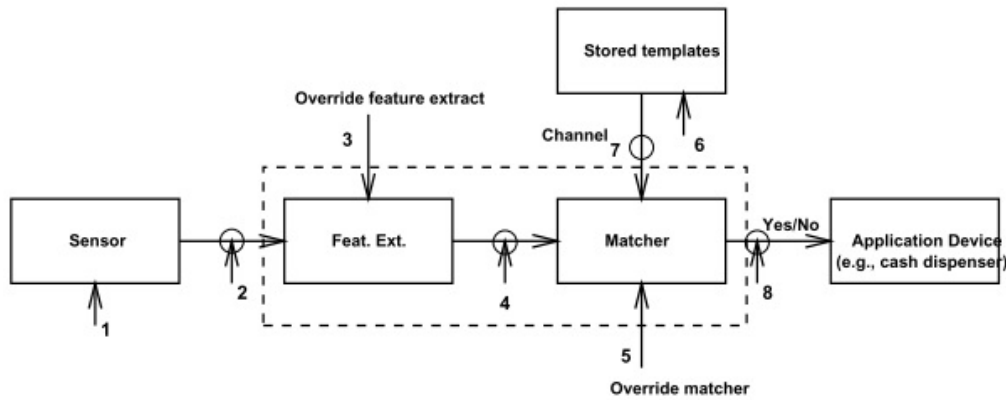


Figure 2.4: Vulnerable points of Biometric Systems [16].

- *Point 3* - A Trojan horse can attack the feature extractor so that it would produce feature sets chosen by the hacker;
- *Point 4* - This attack corresponds to the falsification of the feature representation. After the features have been extracted from the input signal, they are replaced with a different synthesized feature set. Usually the feature extraction and matcher are inseparable, nevertheless, if some data is transmitted to a remote matcher, someone could access the TCP/IP stack inside the computer and change some packets;
- *Point 5* - The matcher can be attacked to always produce an artificially high or low match score;
- *Point 6* - An attacker may try to access the stored templates, which are available locally or remotely, and modify one or more templates in the database in order to allow a fraudulent subject to be authorized into the system;
- *Point 7* - An attack to the channel between the stored templates database and the matcher can result in changes in the original content of the templates that pass through the channel;
- *Point 8* - If the matcher's decision can be overridden with another outcome, the application device will get false results, which can lead to a unwanted access to the system.

The work developed during this dissertation is focused on the first point of attack presented, the direct attack. That way, we will be working with traits, real or fake, that are presented to the sensor of a recognition system. Our purpose is then to classify iris and fingerprints as real or fake.

Some ways of spoofing an iris recognition system at the sensor stage are: by presenting a printed image of an iris, using an artificial mold, using a real iris removed from an enrolled user or using

printed contact lenses. We will focus our attention in this last method since it is quite recent and there are still very few studies that search methods of detecting the fake lenses.

On the other hand, the access to a fingerprint recognition system can be forged by using printed images of a fingerprint, using a real finger removed from an authentic user or by creating a mold of a finger. That can be done with the user cooperation, that is, the user placed his finger in a material capable of creating a mold, or without user cooperation, through capturing a fingerprint let on a surface or object.

In order to reduce the number of successful direct attacks, one or more measures of detecting whether a real or a fake image is being presented to the sensor should be added to the recognition system.

One way of achieving that is by studying the liveness of the submitted trait. Several liveness detection methods have been implemented in biometric systems by adding extra hardware, by using the information already captured by the device, or by using liveness information inherent to the biometric trait [17]. However, adding hardware can be quite expensive so software solutions are the most common ones and thus we decided to use software methods.

2.5.1 Accuracy Measurements

To determine whether a liveness detection method is viable or not, one should assess the performance of its classification system. The classification is usually measured in terms of error rate or accuracy [18].

Two types of error may occur while performing a liveness detection action: a fake image can be labeled as a real one or a real image can be considered as fake.

The implications of these errors in terms of security are weighted differently. Usually, if a real image is classified as a fake one and the access of an authorized person is denied, that can be inconvenient but does not introduce insecurity to the process, whereas if a fake sample is considered as a real one, a potential impostor could have access to whatever was protected by the system, compromising its security. However, there could be also systems where the compromise between the two different types of errors is balanced in such way that the denial of access to real users is more important than the authorization of non-registered users.

In a general way, the error rate is calculated by finding the ratio between the number of misclassified images, that is, the sum of real images considered as fakes and fake images accepted as real, and the total number of images in the testing set (Equation 2.3). The accuracy is precisely the opposite of the error rate, that is, the percentage of correctly classified images (Equation 2.4).

Using this formula, the type of error, i.e. fake accepted images or real rejected images, is not being taken into account, as it only uses the total number of classification errors.

$$\text{Error Rate} = \frac{\text{misclassified images}}{\text{total number of images}} \times 100(\%) \quad (2.3)$$

$$\text{Accuracy} = 100\% - \text{Error Rate} \quad (2.4)$$

Chapter 3

State of the Art

3.1 Iris Recognition and Liveness Detection

3.1.1 Eye Anatomy

The eye (Figure 3.1) is a globular and hollow part of the human body composed by three layers: the internal, external and middle layer [13].

The external layer can also be called fibrous tunic and is constituted by the sclera and the cornea. The middle layer, or uvea/vascular tunic, has the iris and the ciliary body in it; and the internal layer, called nervous tunic, is composed by the retina.

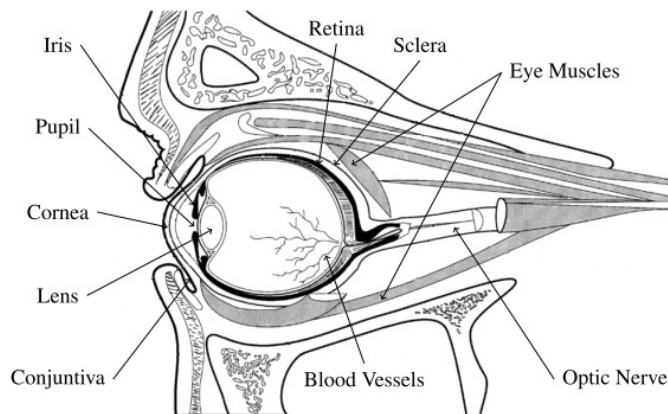


Figure 3.1: Human Eye Anatomy [11].

When observing a human eye (Figure 3.2), in a non-invasive way, three of its features can be seen: the sclera, the pupil and the iris.

The sclera, commonly known as the white area of the eye, is a tough and fibrous tissue that surrounds the eye and aims to protect it, maintain the 3D shape of it and connect it with some of the movement muscles.

The pupil is a black hole located in the center of the eye that allows light to enter the retina. The

iris is the colored ring between the sclera and the pupil, it is made of an elastic tissue and it aims to control the amount of light entering through the pupil [19]. The iris begins to form during the third month of gestation and its structure is complete by the eighth month, although pigmentation continues through the first year after birth. These biological characteristics and the chaotic appearance of the iris patterns turned it one of the most suitable traits for biometric purposes [11].

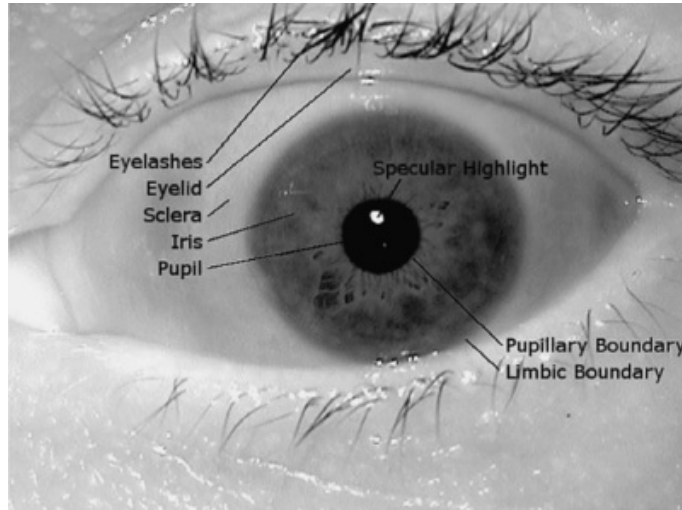


Figure 3.2: Photograph of a Human Eye [20].

3.1.2 Iris Databases

In this section the main characteristics of some available iris databases are described. In the description of each database, the quality of the images and its noise factors as well as the number of real and fake images are presented. Iris databases aim to promote the development of iris recognition and assess the technology's current level of performance.

3.1.2.1 BATH

The University of Bath iris image database presently contains over 16,000 iris images derived from 800 eyes of 400 individuals [11]. The images were taken from students and staff of the University, they are presented in gray scale, have very high quality and contain noise factors related with obstructions due to eyelids and eyelashes, as can be seen in the Figure 3.3.

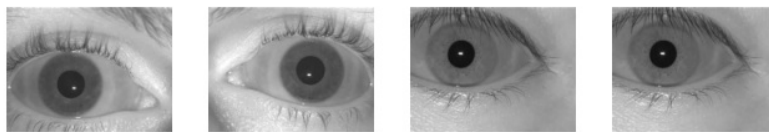


Figure 3.3: Examples of iris images from BATH database [11].

3.1.2.2 CASIA

The latest version of CASIA database, CASIA-Irisv4 [21], contains a total of 54,607 iris images. This database has several similarities with the BATH database (Subsection 3.1.2.1) since its images were also captured under very constrained circumstances thus conditioning the resultant images. All iris images from the CASIA-Irisv4 database are 8 bit gray-level JPEG files, they present homogeneous characteristics and their noise factors are related with iris obstructions. It comprises six data subsets, which were collected or synthesized at different times: CASIA-Iris-Interval, CASIA-Iris-Lamp, CASIA-Iris-Distance, CASIA-Iris-Thousand, CASIA-Iris-Twins and CASIA-Iris-Syn.

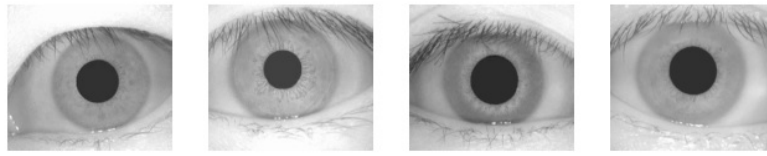


Figure 3.4: Examples of iris images from CASIA database [11].

3.1.2.3 ICE

The ICE database [22] is the database of the contest Iris Challenge Evaluation. The database is constituted of 2,954 images, with a variable number of images per individual. The images from the ICE database have high quality and their noise factors are mostly related to iris obstructions and poorly focused images.



Figure 3.5: Examples of iris images from ICE database [11].

3.1.2.4 WVU

The WVU database [23] was developed by the West Virginia University and it consists of 1,852 images from 380 different eyes.

The images from this DB were captured under less constrained conditions and thus incorporate assorted types of noise, such as iris obstruction, poorly focused images and off-angle images. A few images have some regions affected by specular and lighting reflections which result from their acquisition under a natural environment.

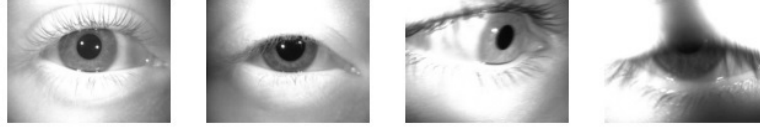


Figure 3.6: Examples of iris images from WVU database [11].

3.1.2.5 UBIRIS.v1

The UBIRIS.v1 database [24] contains 1,877 colored images from 241 subjects and was collected in Universidade da Beira Interior in 2004, in two distinct sections. The set of 10 images from each subject is composed by 5 images from each session.

This DB provides images with different types of noise, simulating the capture with and without user's cooperation, aiming to be a useful resource for the evaluation of iris recognition methodologies.

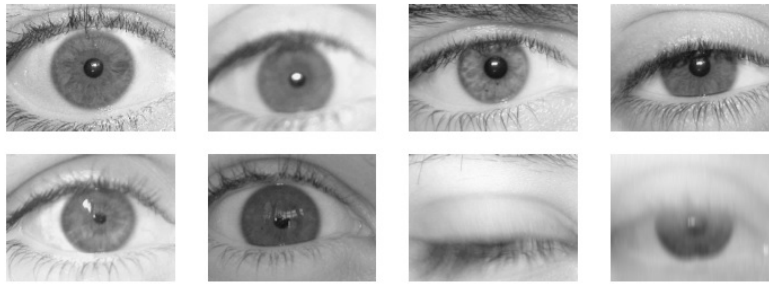


Figure 3.7: Examples of iris images from UBIRIS.v1 database [24].

3.1.2.6 UBIRIS.v2

The UBIRIS.v2 database [25] has 11,102 colored images from 522 subjects and, similarly to the first version of this database, it was collected in Universidade da Beira Interior in two sessions.

The distinguishing points of this DB are the distance used between the capture equipment and the user, the unconstrained acquisition conditions and the several types of noise in the images, such as iris obstructions, lightning and specular reflections, poor focus, partially captured or out-of-image iris, off-angle iris and motion blurred images.

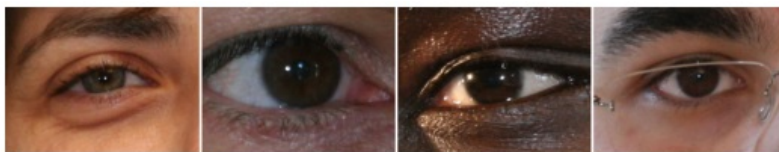


Figure 3.8: Examples of iris images from UBIRIS.v2 database [26].

3.1.2.7 MMU

The MMU database [27] was developed by the Multimedia University and is constituted by 450 images of iris. Afterwards, a new dataset with 995 images was made, MMU2. The images were captured from 100 subjects with different ages and nationalities that provided five images from each eye. Analogous to other databases, MMU contains highly homogeneous images and their noise factors are related with iris obstructions and eye rotation, as can be seen in the second image of Figure 3.9.



Figure 3.9: Examples of iris images from MMU database [11].

3.1.2.8 UPOL

The UPOL database is an iris image database that contains 384 images extracted from 64 subjects, with three iris images per eye. This database was built within the University of Palackého and Olomouc and its images were captured with optometric equipment, leading to very high quality images and maximum homogeneity. A dark circle (Figure 3.10) was added around the iris in all images in order to allow an easier segmentation.

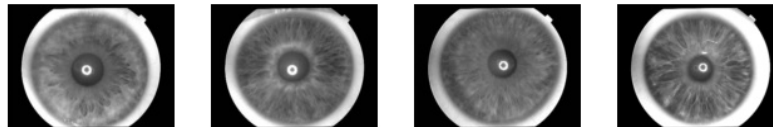


Figure 3.10: Examples of iris images from UPOL database [11].

3.1.2.9 MobBIO

The MobBIO [28] database was created by a group of researchers of the Visual Computing and Machine Intelligence (VCMi) group at INESC Porto and contains biometric data from the face, iris and voice of 105 individuals.

The images are colored and were captured by the back camera of an Asus Transformer Pad TF 300T, with a resolution of 8 megapixels and auto-focus.

Some types of noise factors can be found in this database images such as iris obstructions, glasses reflection and occlusion, reflection occlusion and off-angle iris.



Figure 3.11: Examples of iris images from MobBIO database[28].

3.1.3 Iris Recognition Methods

In this section two classic methods in the iris recognition field are presented. The methods described are the Daugman's and Wildes' methods, considered as pioneers in this area.

3.1.3.1 Daugman's method

In his early work, Professor John Daugman established the main principles of a biometric system based on iris. His method of iris recognition [29] can be decomposed in four main stages (Figure 3.12):

- Iris segmentation
- Normalization
- Feature extraction
- Feature comparison

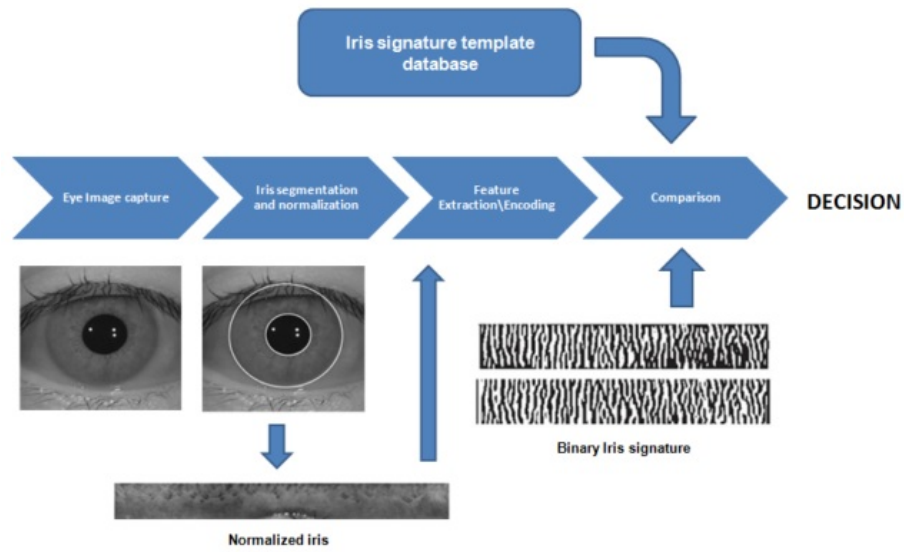


Figure 3.12: Schematic diagram of Daugman's iris recognition method [13].

For the iris localization and segmentation, Daugman proposed an integro-differential operator (Equation 3.1) that searches for the maximum difference between the average intensity of circumferences with consecutive radius values [11].

$$\max_{r, x_0, y_0} \left| G_{\sigma}(r) * \frac{\delta}{\delta r} \oint_{r, x_0, y_0} \frac{I(x, y)}{2\pi r} ds \right| \quad (3.1)$$

In the Equation 3.1, the integro-differential operator I represents the original iris image and G_{σ} is a low-pass Gaussian filter that aims to smooth the image; the r represents the radius and the x_0 and y_0 represent the coordinates of the iris' center.

Next, in order to overcome some limitations concerning different iris' sizes and dilatation or contraction of the iris, Daugman suggested that the next stage should be the normalization, known as the Daugman Rubber Sheet model, which can be observed in Figure 3.13.

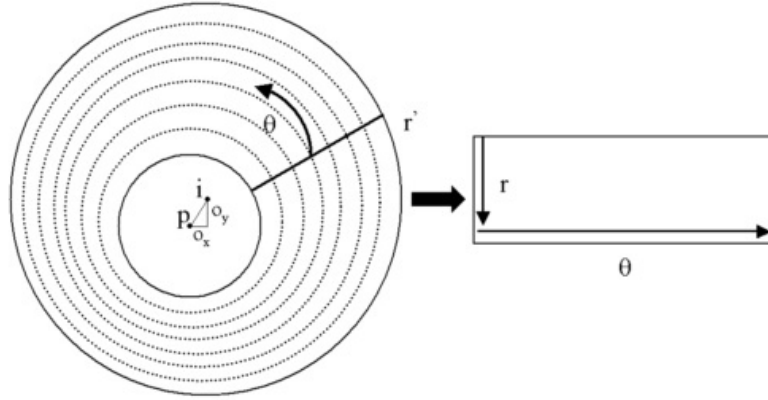


Figure 3.13: Normalization of the iris image through Daugman's Rubber Sheet [11].

Through this model, the images are translated to a dimensionless polar coordinate system and regardless of the iris size or its contraction/dilation, its information is saved in a $n \times \theta$ rectangular image [11, 13, 29].

After the normalization, Professor Daugman suggests using 2D Gabor filters in order to analyze the texture and extract the features. These filters are described through the Equation 3.2.

$$G(x, y) = e^{-\pi \left[\frac{(x-x_0)^2}{\alpha^2} + \frac{(y-y_0)^2}{\beta^2} \right]} \cdot e^{-2\pi i [u_0(x-x_0) + v_0(y-y_0)]} \quad (3.2)$$

where (x_0, y_0) defines the position in the image, (α, β) is the filter width and length and (u_0, v_0) specify the modulation, with spatial frequency $w_0 = \sqrt{u_0^2 + v_0^2}$ and direction $\theta_0 = \arctan(v_0/u_0)$.

The resulting phase response to each Gabor filter results in two bits:

- The first bit is assigned with 1 if the real part of the response is positive or 0 if it is negative;
- The second bit is assigned with 1 if the imaginary part is positive or 0 if it is negative.

This technique aims to lower the computing time and complexity of the algorithm as it results in a binary code for each iris signature and thus the matching process can be performed by simple bit operations. This binarization also allows the application of the Hamming distance as the dissimilarity measurement. Given two binary sets, corresponding to two iris images, with N bits, the Hamming distance can be described as:

$$HD(A, B) = \frac{1}{N} * \sum_{i=1}^N a_i \otimes b_i \quad (3.3)$$

where $A = \{a_1, \dots, a_N\}$ and $B = \{b_1, \dots, b_N\}$, resulting in a Hamming distance of 0 for two equal images and 1 for different ones.

3.1.3.2 Wildes' method

Wildes' [30] method for iris recognition can be divided in three parts (Figure 3.14):

- Image acquisition
- Image segmentation
- Pattern matching

Wildes considered that, since the iris' dimension is so small (about 1 cm in diameter), the acquisition of its image should be a major concern when developing iris recognition systems. In his work, he emphasizes the importance of obtaining images with high resolution, sharpness and good contrast in the iris pattern. He also enunciates that the images should be well framed and the artifacts and obstructions should be eliminated.

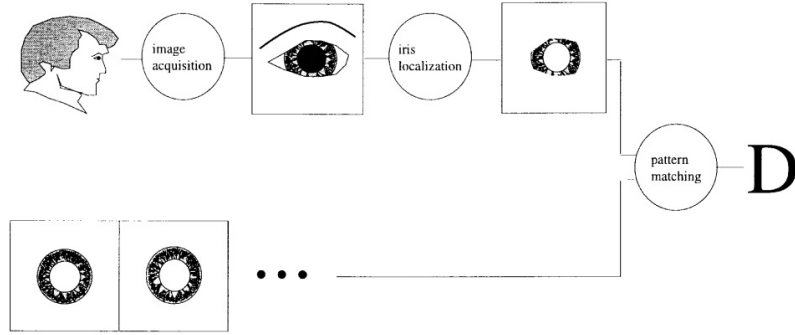


Figure 3.14: Schematic diagram of Wildes' iris recognition method [30].

As the acquisition module captures larger images which contain not only iris but also regions of its surroundings, the location of the iris is critical in this process. The image segmentation is accomplished in two steps: first, the intensity information of the iris image is converted into a binary edge map. Then, the edge points vote to instantiate particular contour parameter values and the edge map is recovered through a gradient-based edge detection (Equation 3.4) which comes down to thresholding the magnitude of the image intensity gradient convolved with a two-dimensional Gaussian Kernel G .

$$|\nabla G(x, y) * I(x, y)| \quad (3.4)$$

where

$$\nabla \equiv \left(\frac{\delta}{\delta x}, \frac{\delta}{\delta y} \right) \quad (3.5)$$

and G is a 2D Gaussian Kernel described by:

$$G(x, y) = \frac{1}{2\pi\sigma^2} e^{-\frac{(x-x_0)^2 + (y-y_0)^2}{2\sigma^2}} \quad (3.6)$$

The limbic boundary detection is obtained through a maximization process, similar to the one used in Daugman's method, using an integro-differential operator. The parameters used for this

maximization are then used by a scoring method called Circular Hough Transform (CHT):

$$H(x_c, y_c, r) = \sum_{j=1}^n h(x_j, y_j, x_c, y_c, r) \quad (3.7)$$

where x_c , y_c and r are the parameters used for the maximization and

$$h(x_j, y_j, x_c, y_c, r) = \begin{cases} 1, & \text{if } g(x_j, y_j, x_c, y_c, r) = 0 \\ 0, & \text{otherwise} \end{cases} \quad (3.8)$$

with

$$g(x_j, y_j, x_c, y_c, r) = (x_j - x_c)^2 + (y_j - y_c)^2 - r^2 \quad (3.9)$$

The global maximum of the H array is identified as the most probable candidate to represent the limbic boundary, that is, the iris' borders.

Lastly, the final step is to settle if the captured pattern matches one of the previously stored. This task can be divided in four parts:

- **Alignment:** spatially align the new iris pattern with candidate previously stored;
- **Representation:** choose a representation of the aligned patterns that makes their dissimilarities noticeable;
- **Comparison:** evaluate the excellence of the match;
- **Decision:** decide if the patterns, both the recently acquired and the previously stored, derive from the same iris.

Table 3.1 outlines the advantages and disadvantages of Wildes' method in comparison with Daugman's.

Advantages	Disadvantages
Less intrusive light source Removal of specular reflection Segmentation is more stable to noise disturbances Capable of finer distinctions Better adaptability to real world situations	Complex acquisition system Smaller sensitivity to some details Less compact representation of iris features High computational cost

Table 3.1: Advantages and disadvantages of Wildes' method. Adapted from [13].

3.1.4 Commercially Available Solutions

Nowadays, the implementation of iris recognition systems is becoming usual and some of these systems can already be seen at airports, border control and social security services or even at private companies, which use them to give access to a room or area. Here some of the commercially

available systems are presented :

IRIS - Iris Recognition Immigration System

IRIS [31] was implemented by the United Kingdom border agency in order to regulate the flow of people entering the UK, namely frequent travelers. This system was used by the following airports: Heathrow, Manchester, Birmingham and Gatwick; however, since this is already an old system, the UK border agency decided to decommission it.

IrisGuard's Homeland Security Border Control

This system is used by the United Arab Emirates' Expellee Tracking and Border Crossing Control System in all its 17 air, land, and sea ports since 2001, revealing some optimistic results relative to false matches as none was reported, from 2001 to 2004, despite of 2.7 thousand millions iris daily comparisons [32].

India's UID Program

The Unique ID program [33] is the Indian's unique identification number which is linked with biometric details – fingerprints and iris. They use this system to eliminate redundant records from their database and simplify the authentication process since the lack of some identification documents by the poorest residents is quite common.

CANPASS Air and NEXUS

NEXUS pass is a binational boarding crossing pass for faster US Canada and USA border crossing [34]. Travellers with NEXUS pass can cross the border without being subject to regular questioning by customs and immigration officers [35]. People applying for the card must have an iris scan during an interview and some high-resolution iris images are taken [36].

CairoAmman Bank System

CairoAmman was one of the the first companies in the banking section to use an iris recognition system in their offices and ATMs. This iris recognition system is available at more than sixty ATMs and more than thirty seven offices [37].

Bank United System

The Bank United Corporation from Houston, USA, installed an iris scanning system at three of its ATMs and researched whether it was well accepted by the clients or not. The response to the survey, made by an independent research was positive, as 98% of the users reported their experience as a good one [38].

Based on the positive response by the clients, they decided then to install the system at sixty ATMs in supermarkets across Texas [39].

Venerable Bede School - Impact

Venerable Bede School in Ryhope, England, uses an iris recognition system instead of ID cards for its students. The system used is called “Impact”, it was implemented in the fall of 2003 and is composed by an iris recognition camera which is integrated into a catering system. This way, students are identified and their meals are automatically charged to an account. They can also borrow library books or access restricted areas in the school, if they have permission [39].

3.1.5 Iris Liveness Detection

3.1.5.1 Illegal use of iris recognition systems

The fact that the human iris has such unique features makes them useful in biometric systems. Nevertheless, as any other automated recognition technique, systems using iris as a biometric template may be spoofed and illegally used. Some of the most common ways of forging an iris recognition system are [40]:

- *Use of an eye image* - e.g. photographs, video signal, screen images or paper print images (Figure 3.15);
- *Use of an artificial eye* - e.g. eye made of plastic, glass, silicon;
- *Use of a natural eye (user)* - i.e. forcing an individual to use the system;
- *Capture/Replay attack* - e.g. eye image or iris code template;
- *Use of a natural eye (impostor)* - i.e. eye removed from body or printed contact lenses (Figure 3.16).



Figure 3.15: Use of printed iris images in a biometric system [15].

One of the most popular and convenient technique, out of these falsification ones, is the use of printed contact lenses. If an individual enrolls into the system using cosmetic contact lenses,

anyone wearing the same lenses can be authorized into the system, even unintentionally. Besides that, the texture of someone's iris can be printed into contact lenses with the purpose of illegally accessing an iris recognition system [41].

Since the use of cosmetic contact lenses as a spoofing technique is a subject quite recent and has not been fully researched, the initial part of the development of this dissertation will give some attention to iris liveness detection methods directed to the identification of fake iris images wearing cosmetic contact lenses.

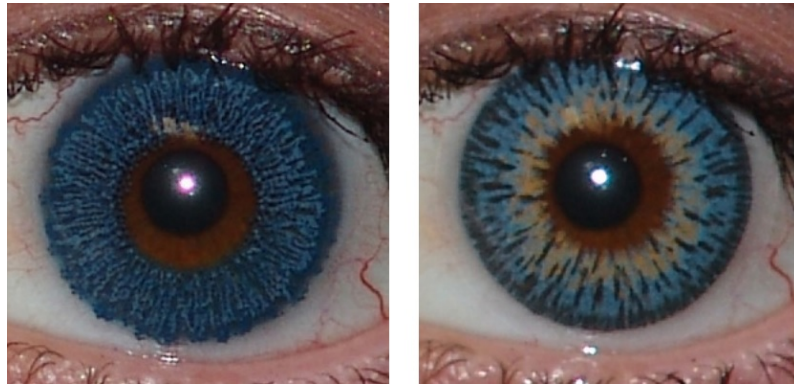


Figure 3.16: Examples of cosmetic contact lenses [42].

3.1.5.2 Iris Liveness Detection Methods

Detecting whether an iris is alive or not, promotes the robustness and reliability of a recognition system against direct attacks and helps obtaining a system with a higher security level [43].

The liveness detection methods can be divided in four categories based on physical characteristics of the chosen biometric trait, liveness data and measurement times [44]:

- Simultaneous measuring model: biometric and liveness data are simultaneously obtained from different physical characteristics;
- Same biometric measuring model: biometric and liveness data are obtained from the same physical characteristic, but not at the same time;
- Independent measuring model: biometric and liveness data are obtained from different physical characteristics, in different times;
- Perfect matching model: both biometric and liveness data are obtained at the same time from the same physical characteristic. This category is considered the ideal configuration.

These techniques can also be divided into two classes:

- **Software-based techniques:** fake irises are detected once the sample has been acquired by the sensor and the detection of its liveness is done using the image captured;

- **Hardware-based techniques:** an additional device is added to the sensor in order to detect the liveness of the iris by measuring some particular properties. Daugman [45] states that this type of detection can be done based in two types of eye behavior – voluntary or involuntary behavior. The voluntary moves are those where the user moves the eyes or blinks them according to system indication. The involuntary ones happen when the eye moves without the user's demand, as the pupil oscillation, dilatation or contraction as a response to light.

Even though hardware-based approaches are usually more efficient, software-based ones are less expensive and less intrusive for the user and thus are commonly favored. Next, some software-based methods are presented.

Daugman [46] and Tan et al. [47] proposed a software-based method of detecting iris liveness via frequency analysis, through FFT's – Fast Fourier Transform. However, this technique can only be used for printed iris detection as it uses the frequency aspects of a printed image contrasting with a living iris.

He et al. [48] suggested another method for iris liveness detection via statistical texture analysis for detecting the use of contact lenses. In this method, four features based on gray level co-occurrence matrix (GLCM) and properties of statistical intensity values of image pixels are extracted and a support vector machine is used for classification.

Detecting iris edge sharpness is another possible measure for iris liveness detection. When contact lenses are used, fake iris edge is sharper than the edge of a living one [41].

Wei et al. [41] also proposed the use of texture analysis to detect contact lenses but in their work Iris-Textons are learned and used for texture representation.

The potential of quality assessment to identify real and fake iris images was analyzed in [43] and has also been tested for spoofing detection in fingerprint recognition systems.

The main point of a software-based liveness detection process is to identify a set of discriminant features that allow the construction of an appropriate classifier that provides the probability of an iris being alive or not, based on the extracted set of features.

3.1.5.3 Databases with fake samples

In order to test iris liveness detection methods, databases with false samples are needed. Since some work will be done in detecting the use of cosmetic contact lenses, two of the presented databases have fake samples using colored contact lenses and will be used later on to test the implemented algorithms.

CLARKSON

This database was made available for the contestants of the LivDet-2013 challenge [49]. It contains 270 images of real iris and 400 of fake ones. All the fake samples are images of iris with contact lenses, with a total of 14 types of lenses. The data was acquired through video (100 frames with focus variation) and two types of lighting are present in the database.



Figure 3.17: Examples of iris images from CLARKSON database. Images a) and b) are real and c) and d) are fake images.

NOTRE DAME

The Notre Dame [50] database contains iris images:

- with cosmetic contact lenses;
- with clear soft lenses;
- without contact lenses.

All images are 480 x 640 in size and were acquired under near-IR illumination, in two different periods – the soft lens and no lens data was acquired from 2008 to 2010 and the cosmetic contact lens images were acquired in 2012.

The total image training database contains 1000 images without contact lenses, 1000 images with soft contact lenses and 1000 with cosmetic contact lenses, leading to a total of 3000 images.

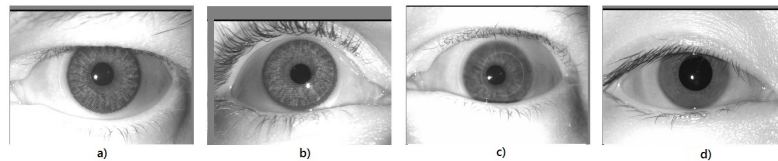


Figure 3.18: Examples of iris images from NOTRE DAME database. a) and b) correspond to images with cosmetic contact lenses; image c) has soft contact lenses and d) corresponds to an image without lenses.

WARSAW

The Warsaw [51] database contains 228 real images and 203 fake images. The fake images were obtained by printing the original ones. This database was made available for the participants in the LivDet-2013.

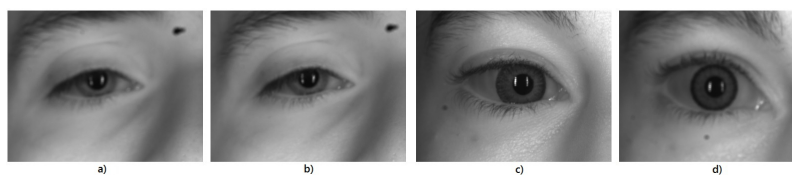


Figure 3.19: Examples of iris images from WARSAW database. a) and b) correspond to real images; images c) and d) corresponds to images with cosmetic lenses.

MobBIOfake

The MobBIOfake [52] database contains 800 iris images and its 800 correspondent fake images. The fake images were printed images from the original database, captured with the same device, in similar lighting conditions.

This database was constructed upon the MobBio Database (see Section 3.1.2.9) which is a multi-modal database that contains samples of voice, face and iris.

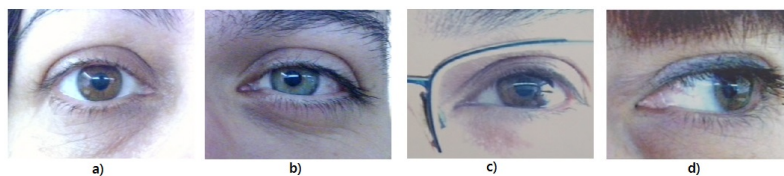


Figure 3.20: Examples of iris images from MobBIOfake database. Images a) and b) are real images and c) and d) are fake ones.

BIOSEC

The Biosec [53] database was created in the Polytechnic University of Madrid (UPM) and Polytechnic University of Catalunya (UPC) and contains both real and fake iris images. The images were taken in unconstrained conditions, in order to simulate a real situation, with a LB IrisAccess EOU3000 sensor. To build the fake part of the DB, the original images were preprocessed and printed in a paper, using a commercial printer. Then, the printed images were presented to the sensor, obtaining the fake samples.

The Biosec database contains 800 fake images and its correspondent real images. Fifty people participated in the image acquisition process which took place in two different occasions [15].

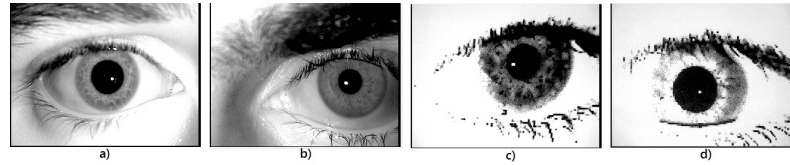


Figure 3.21: Examples of iris images from BIOSEC database. a) and b) correspond to real images and c) and d) to fake images.

3.2 Fingerprint Recognition and Liveness Detection

3.2.1 Fingerprint Anatomy

Fingerprints are small lines/ridges and valleys in the skin of fingertips. Their configuration do not change throughout life (except if an accident, such as a burnt, happens) and are formed at around seven months of fetus development due to a combination of genes and environmental factors. [18, 54]

The environmental factors of the fingerprint formation result in such variations that it is considered impossible to have two fingerprints looking exactly alike [55, 18]. However, their patterns are not completely random and can be divided in three types: arches, loops and whorls (Figure 3.22).

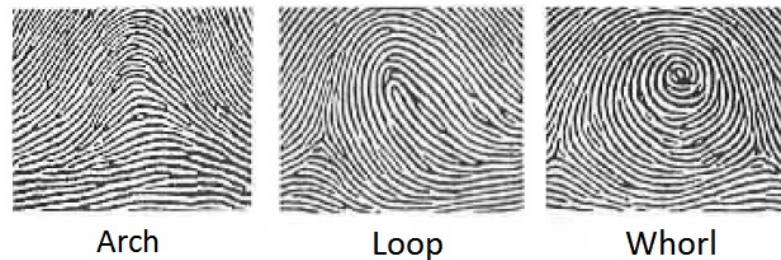


Figure 3.22: Three main fingerprint pattern types. [54]

These three types of patterns can also be sub-divided into more detailed groups: right/left loops, plain/narrow arches or spiral/concentric whorls. [55]

Fingerprints can also be observed at three levels of detail: the global, local and very-fine levels. At the global level singularity points such as core and delta can be found (Figure 3.23). At the local level minutiae points can be observed. The two most common ones are ridge termination and ridge bifurcation, but others can be seen in Figure 3.23. Finally, at the very-fine level one can see essentially sweat pores. [54]

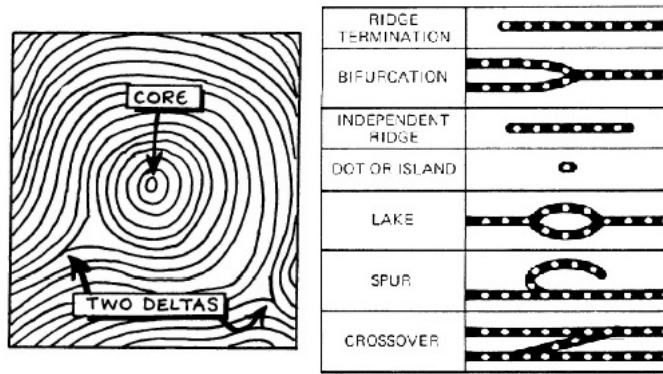


Figure 3.23: Core and delta points on a fingerprint illustration and fingerprint minutiae details (Adapted from [54]).

3.2.2 Fingerprint Databases

As fingerprints have been used to identify people for quite a long time, plenty of fingerprint databases have been built. However, most of them are unavailable or private due to security concerns. That is, for instance, the case of the civil registration databases or police identification databases.

In this section we present a couple of databases used for academic and research purposes.

3.2.2.1 NIST databases

The National Institute of Standards and Technology has built several fingerprint databases over the last years:

- NIST DB 4 [56],
- NIST DB 9 [57],
- NIST DB 10 [58],
- NIST DB 14 [59],
- NIST DB 24 [60],
- NIST DB 27 [61].

NIST DB 4, 9, 19 and 14 contain a large sets of images scanned from rolled inked impressions. NIST DB 27 contains 100 video sequences from 10 individuals. This database was mostly used to study the effect of finger rotation and plastic distortion. NIST DB 27 contains latent fingerprints and their corresponding rolled impressions. Minutiae data was manually extracted by experts and is also provided with the database [18].

3.2.2.2 FVC2006

This database was made available for the participants in the Fingerprint Verification Competition 2006 and comprises 1800 fingerprint images [62]. Four datasets were created using three different scanners and a synthetic generator.

Each dataset has 150 fingers, with 12 samples per finger, saved in an uncompressed format.

Data collection was performed without deliberately introducing exaggerated distortion, rotations, etc. and the volunteers were simply asked to put their fingers on the acquisition device.

Before that, three other competitions and databases were made: FVC 2000, 2002 and 2004.



Figure 3.24: Examples of fingerprint images from FVC2006 database [54].

3.2.3 Fingerprint Recognition Methods

Although some fingerprint recognition techniques directly compare images through correlation-based methods, most of the fingerprint recognition and classification algorithms employ a feature extraction stage [18]. For example, some preprocessing, segmentation and enhancement steps are often performed to simplify the task of minutiae extraction. For instance, Sherlock et al's [63] propose fingerprint enhancement through Fourier filtering.

Figure 3.25 presents three possible fingerprint recognition methods.

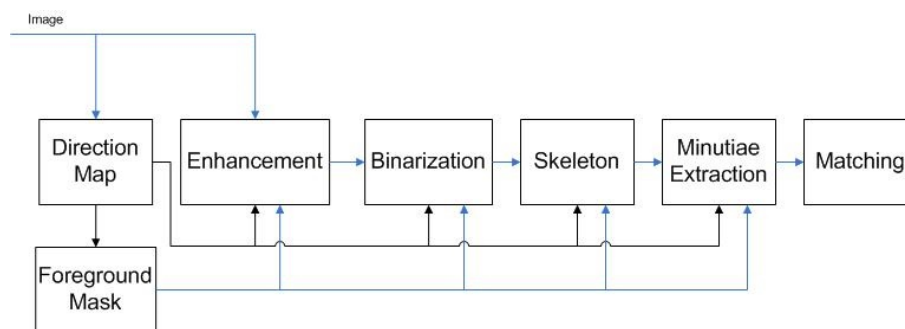


Figure 3.25: Fingerprint recognition system block diagram.

A direction map (Figure 3.26) is built by finding the local ridge orientations of pixels. The local ridge orientation of a pixel (x, y) is the angle that the fingerprint ridges crossing a small neighborhood, centered in that pixel, forms with the horizontal axis.

As fingerprint ridges are not directed, the angle corresponds to an unoriented direction in the range of $[0...180^\circ[$. Instead of computing local ridge orientation at each pixel, most of the fingerprint methods estimate the local ridge orientation at discrete positions, reducing computational efforts [18].

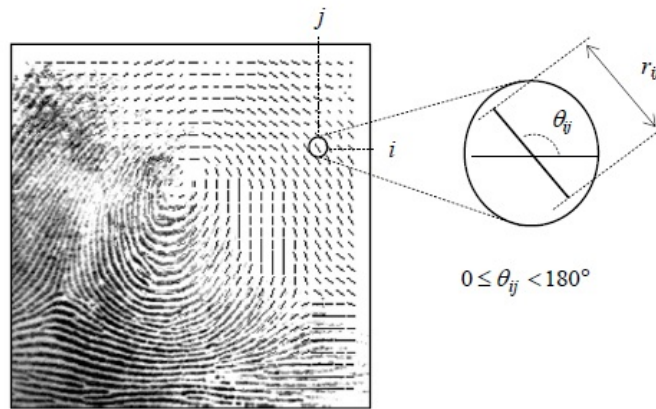


Figure 3.26: A fingerprint image faded into the corresponding direction map [18].

The simplest binarization approach uses a global threshold and works by setting the pixels whose gray-level is lower than the threshold to 0 and the remaining pixels to 1. However, different portions of an image may have different contrast and intensity and thus a single threshold for the entire image may not be sufficient for a correct binarization. Some binarization methods were proposed by Abutaleb et al. [64] and Zhang et al. [65] and through binarizing the image, a skeleton image is obtained (Figure 3.27).



Figure 3.27: Fingerprint image and corresponding binarized skeleton[18].

While some authors propose minutiae extraction methods that need previous binarization, others use approaches that work directly with gray-scale images, as binarization is time consuming and some information may be lost during its process.

A fingerprint matching algorithm compares two given fingerprints and returns either a degree of similarity or a binary decision [18]. There are several factors that should be taken into account when performing fingerprint matching and that can influence its result, like displacements, rotations, partial overlaps, distortions, pressure, skin conditions and noise.

Fingerprint matching techniques can be divided into three groups:

- **Correlation-based matching:** the correlation between two fingerprint images' pixels is computed for different alignments. One example of a correlation-based matching is the one proposed by Hatano et al.'s [66];
- **Minutiae-based matching:** Minutiae are extracted from the two fingerprint images and stored as sets of points in a two dimensional plane. By comparing the two stored matrices, the method tries to find an alignment between them so that it results in the maximum number of minutiae pairings. Jea et al's [67] proposed a method for this type of matching methods;
- **Non-Minutiae feature-based matching:** comparison of fingerprints in terms of features extracted from the ridge pattern. The most commonly used features are: size of fingerprint and external silhouette; number, type and position of singularities; global and local texture information; geometrical attributes and spatial relationship of the ridge lines; level 3 features (e.g. sweat pores). For instance, Zhang et al's [68] proposed a method based in local texture information.

3.2.4 Fingerprint Sensors

The traditional way of obtaining a fingerprint is the called off-line fingerprint acquisition, also called "ink-technique". In this technique a person's finger is stained with black ink and pressed or rolled on a paper. That paper is then scanned by a regular scanner obtaining then a digital image of the fingerprint [18].

However, with the growth of demand and technological development, the most used technique is the live-scan acquisition in which digital images are obtained directly through a scanner. This development has also allowed the creation of smaller scanners, with lower prices, that can even be integrated into laptops, smartphones or mice. [54].

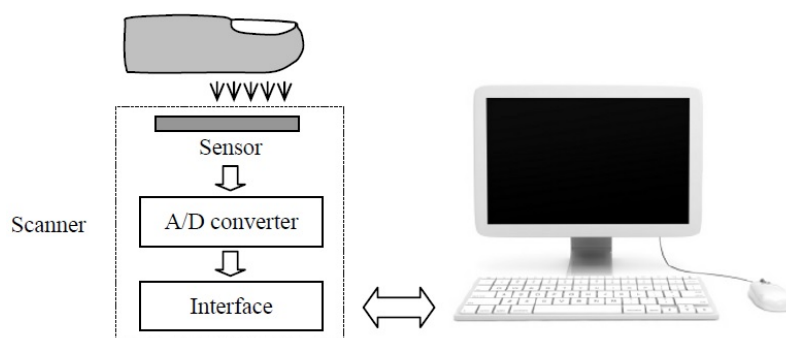


Figure 3.28: Typical structure of a fingerprint scanner [18].

Typically, a sensor has the following structure: it reads the ridge pattern in the surface of a finger, converts the analog reading to a digital form and an interface module communicates and sends the images to external devices (e.g. a personal computer). This structure is shown in Figure 3.28. Currently available scanners can be classified as *multi-finger*, if more than one finger can be acquired at the same time, or *single-finger*, if only one finger at a time can be acquired (See Figure 3.29).

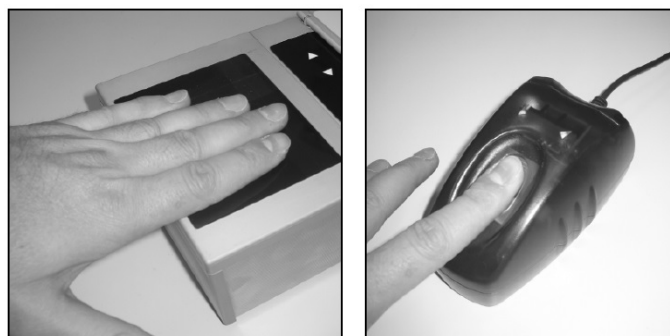


Figure 3.29: Example of fingerprint scanners. The left image represents a multi-finger scanner and the right image represents a single-finger scanner [18].

Fingerprint images can also be stated as *plain*, *rolled* or *swept* considering the type of scanner used (Figure 3.30). Although most scanners acquire plain impressions, some can also obtain rolled ones, which provide more information than plain images. On the other hand, swept images can be obtained using sweep scanners, which have the width of a finger but only a couple of pixels of height, reducing the cost of its manufacturing. However, this type of scanner has some drawbacks such as the learning time that a user needs to learn how to sweep the finger correctly and the time consumed to reconstruct the fingerprint image from the slices acquired.

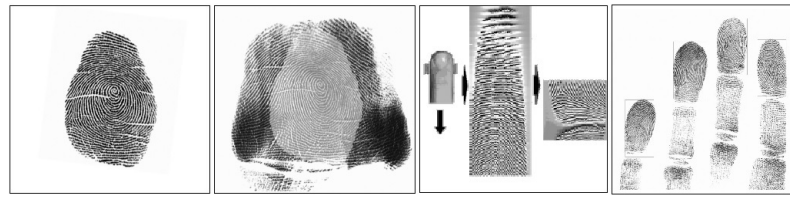


Figure 3.30: Examples of plain, rolled, swept and multiple fingerprints (Adapted from [18]).

In terms of live-scan fingerprint sensing, they can be sub-grouped in three categories: *optical*, *solid-state* and *ultrasound* sensors, being the optical and solid-state the most popular ones [18, 54].

3.2.4.1 Optical Sensors

Optical sensors can stand temperature fluctuations, are low cost and have better image quality than other types of sensors. However, they have some issues when dealing with damages, dirt or latent prints. Next we present some types of optical sensors:

Frustrated Total Internal Reflection (FTIR)

When a subject places his finger in this type of sensor, the finger will touch the top side of a prism made of plastic or glass (Figure 3.31). Only the ridges will be in contact with the surface and there will be a gap between the sensor surface and the valleys.

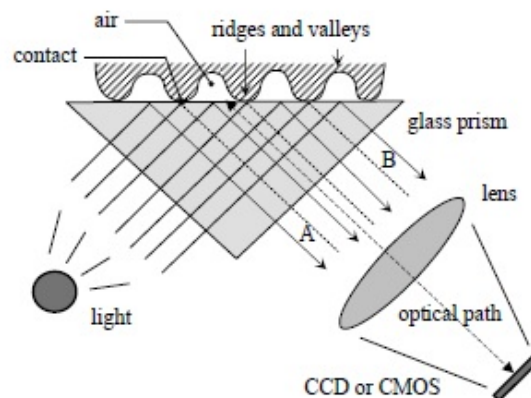


Figure 3.31: FTIR fingerprint acquisition [18].

One side of the prism is usually illuminated through a diffused light (e.g. LEDs). This light enters the prism and is reflected by the valleys (and absorbed by the ridges). As only the valleys are reflected, it is possible to acquire an image of the fingerprint through the caption (with a CCD or CMOS image sensor) of the light rays that exit the prism at its right side.

It is also possible to use a sheet prism made of a number of “prismlets” adjacent to each other instead of a single prism, in order to reduce the size of the sensor, nevertheless, this solution reduces the quality of the images obtained.

The main advantage of this sub-type of sensor is that since it uses three dimensional information, it is difficult to spoof the sensor by using a flat printed image of a fingerprint [18, 54]

Optical Fibers

Instead of using a prism and a lens, this sub-type uses a fiber-optical plate. The finger is in contact with the upper side of the plate, having a CCD or CMOS on the opposite side, which receives the light conveyed through the fiber-optical plate (Figure 3.32). Although the size of the scanner can be smaller, the size of the sensor has to cover the whole sensing area, which may result in increased costs of production [18, 54].

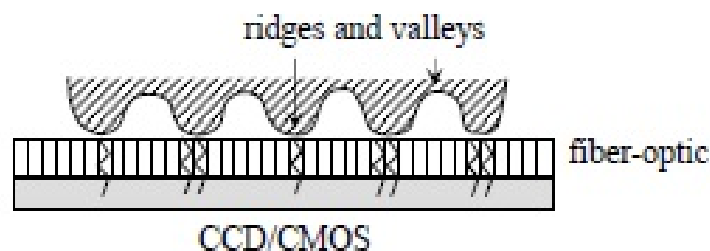


Figure 3.32: Optical-fibers fingerprint acquisition [18].

Electro-optical

This type of sensors have two main layers. The first layer contains a light - emitting polymer that when polarized with the proper voltage, emits light that depends on the potential applied on one side (Figure 3.33).

When a finger is placed on the sensor, the potential applied by the ridges and valleys (and consequent emitted light) is not the same, as ridges touch the polymer and valleys do not. That allows a luminous representation of the fingerprint pattern.

The second layer consists of a photodiode array which receives the light emitted by the polymer and converts it into a digital image.

Scanners using this technology are still behind FTIR in terms of image quality [18, 54].

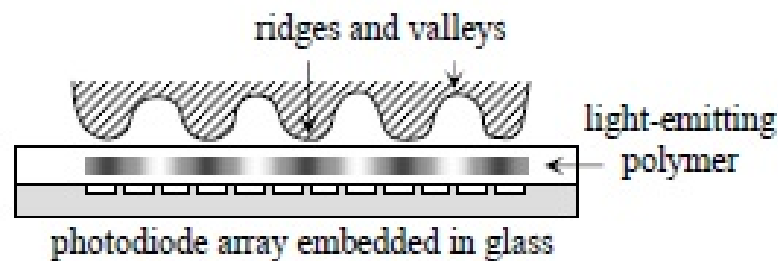


Figure 3.33: Electro-optical fingerprint acquisition [18].

Direct Reading

These sensors are called touchless as the finger is not in contact with any surface. These devices use a high quality camera to focus on the fingerprint but it is very challenging to obtain well-focused and high-contrast images [18, 54].

Multispectral imaging

This sensor captures several images of the same finger using different wavelengths of light, illumination orientation and polarization conditions. The resulting data can generate a single fingerprint image.

This type of sensor is considered more robust than others but it is more complex and expensive and thus it is not the conventionally adopted scanner [18].

3.2.4.2 Solid-state Sensors

Solid-state sensors are also called silicon sensors and generally consist of an array of pixels, where each pixel is a very small sensor itself. They were designed to overcome some problems such as size and production cost.

Capacitive sensors

It is a two-dimensional array of micro-capacitor plates embedded in a chip. In this case, the skin of the finger works as the other plate of the micro-capacitor (Figure 3.34).

Small charges of electricity are created between the finger's surface and each of the silicon plates. The magnitude of these electrical charges depends on the distance between the ridges or valleys and the capacitance plates. These differences can then be used to obtain an image of the fingerprint.

These sensors, like the optical ones, can not be spoofed by photographs or printed images. However, there are a number of disadvantages that should be taken into account, such as: they have a small sensor area which require more careful enrollments; electrostatic discharges from the fingerprint may cause large electrical fields that can damage the device: the silicon chip needs to be

protected from some chemical substances that may be present in finger perspiration[18, 54].

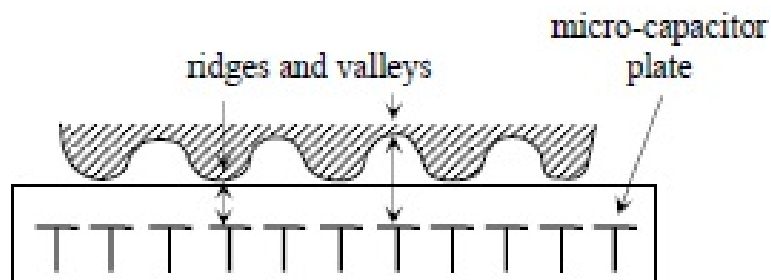


Figure 3.34: Capacitive fingerprint acquisition [18].

Thermal sensors

Thermal sensors are made of pyro-electric material. This material generates current based on temperature differentials. The difference between the temperature of the skin (of the ridges) and the air (in the valleys) is used to obtain the fingerprint image.

These sensors are usually maintained at a high temperature to increase the difference between the sensor surface and the skin of the finger [18, 54].

Electric Field sensors

It creates a fingerprint image from below the top layer of the skin, avoiding the calluses, cuts and dirt that the finger might have. It consists of a drive ring and a matrix of active antennas. The ring generates a radio frequency sinusoidal signal and the antennas receive the signal transmitted by the drive ring and modulated by the subsurface of the skin [18, 54].

Piezoelectric sensors

Piezoelectric sensors are also called pressure-sensitive sensors. Its surface is made of a non-conductive dielectric material that generates current according to the pressure applied by the finger.

The distinct pressure applied by the valleys and the ridges results in different amounts of current [18, 54].

3.2.4.3 Ultrasound Sensors

An ultrasound sensor is based on sending acoustic signals toward the fingerprint and capturing the echo signal. This echo signal is then used to compute the depth image of the fingerprint. In order to perform that, this type of sensor contains two main components: a transmitter and a receiver (Figure 3.35). Even though it is known that ultrasound is probably the most accurate type of sensor for fingerprint recognition, its cost and size still largely influences its use [18, 54].

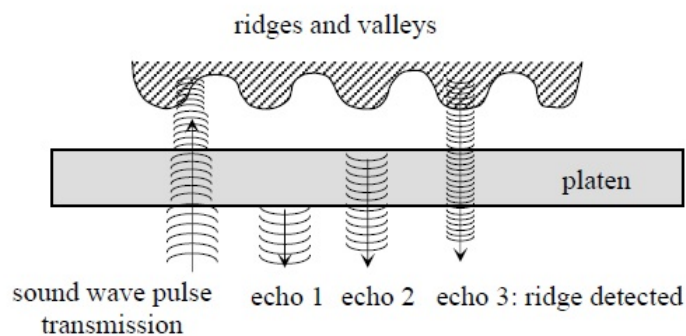


Figure 3.35: Ultrasound fingerprint acquisition [18].

3.2.5 Fingerprint Liveness Detection

3.2.5.1 Fake Fingerprints Acquisition

One of the main problems of fingerprint recognition systems, or biometric recognition systems in general, is that they can be spoofed by using fake samples of the biometric trait used in a specific system. This samples could be acquired with or without user cooperation.

With user cooperation, an authorized user may help an hacker to create a clone of his fingerprint. In order to obtain a fingerprint without the cooperation of its correspondent individual, it is necessary to obtain its print from a glass or other surface. Those marks left on surfaces are called latent fingerprints [18, 69].

Latent fingerprints can be painted with a dye or powder and then “lifted” with tape or glue. However, these prints are, usually, low quality as they can be incomplete or smudged and thus are not very accurate.

The easiest way of creating a fake sample is by printing the fingerprint image into a transparent paper. However, a more successful method is to create a 3D fake model with the fingerprint stamped on it. This can be done by creating a mold that is then filled with a substance (silicon, gelatin, Play-Doh, wax, glue, plastic). This mold is used to create a thick or thin dummy (Figure 3.36) that an intruder can use.

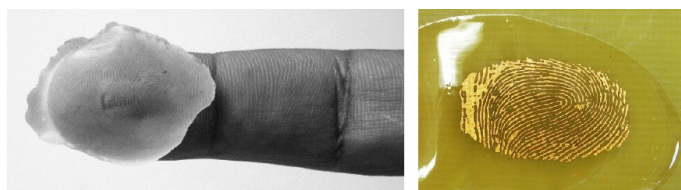


Figure 3.36: Finger model and mold (Adapted from [18, 54]).

3.2.5.2 Liveness Detection Methods

Detecting the liveness of a fingerprint is even harder than detecting the liveness of an iris, as both the material used in the fake models and the epidermis of a finger are not alive.

Just as with iris, liveness detection can be performed through additional hardware or by processing the image obtained. Hardware-based solutions try to detect the liveness of the fingertip by measuring some physical characteristics such as blood pressure, temperature or pulse. These solutions have the disadvantage of being expensive and thus we will confine the study of liveness detection methods to software-based approaches.

Ghiani et al. [70] propose the use of Binarized Statistical Image Features (BSIF) to detect the vitality of fingerprints. This approach has already been tested for face recognition and texture classification and they propose to test it in fingerprint recognition.

Their goal is to obtain statistically meaningful representation of the fingerprint data by learning a fixed set of filters from a small set of images. They also claim that through learning, it is possible to adjust the descriptor length to the unusual characteristics of a fingerprint.

Ghiani et al. tested this algorithm with the four LivDet2011 [71] datasets, obtaining promising results. However, there are still some problems with this algorithm, such as finding the right window size or the length of the binary string that results from the application of the filters to the image.

The same authors of the previous algorithm, Ghiani et al., have also proposed another method for liveness detection by using Local Phase Quantization (LPQ) [72].

The Local Phase Quantization is a blur insensitive texture classification method. As it is able to represent all spectrum characteristics of images in a compact feature representation, avoiding redundant or blurred information, the authors believe that it could be used in this field.

They used the four data sets collected for the Second International Fingerprint Liveness Detection

Competition (LivDet11) [71] to test the algorithm and obtained results almost equivalent to when Local Binary Patterns (LBP) [73] are used.

Diego Gragnaniello et al. [74] investigate the use of a local discriminatory feature space, called Weber Local Descriptor (WLD) for fingerprint liveness detection. This descriptor consists of two blocks: differential excitation and orientation. These are then evaluated for each pixel of the image and concatenated into an histogram that is used to build the discriminatory features.

A linear kernel SVM classifier is then used to classify the images.

These authors have tested this method with both LivDet2009 [75] and LivDet2011 [71] datasets and propose the combination of this method with the Local Phase Quantization (LPQ) [72] in order to obtain better results.

Warwante et al. [76] studied how the Wavelet transform can be applied to fingerprint verification. In this work, it is stated that Wavelet analysis can help minimizing the effect of ridge and valley pattern when estimating the surface coarseness because it allows the study of the input image at different scales.

They have created a high resolution database to which they then applied the proposed algorithm. Although they obtained positive results, one can not say that the same would occur with images with less quality.

In [77], Tan and Schuckers propose a new method for fingerprint liveness detection based on ridge signal analysis and valley noise analysis. They aim to quantify perspiration patterns along ridge in live samples and quantify noise patterns along valleys in fake samples.

Their results show that the performance can reach 99.1% of correctly classified images.

They have also proposed another method based on the statistics of Wavelet signal processing [78] aiming to detect the perspiration phenomenon using only a single image.

Galbally et al. [79] use quality related features in their liveness detection work. The extracted features are ridge strength, ridge continuity and ridge clarity. They claim that those features can be extracted from the following quality measures: local angle, power spectrum and pixel intensity. This study presented an overall rate of 90% correctly classified samples, tested on a challenging database comprising over 10,500 real and fake images. This large database is created from the images of LivDet2009 [75] and ATVS [80] databases.

Ojala et al.'s [73] approach is based on Local Binary Patterns (LBP). It is known that a LBP's histogram can be a powerful texture feature and thus can be used to determine whether a fingerprint is real or fake. Even though this study was published in 2002, it is still a very actual method with results comparable to newer solutions.

3.2.5.3 Databases with fake samples

LivDet 2013 - Fingerprint Liveness Detection Competition 2013

This database was made available for the contestants of the LivDet 2013 [81]. Its images were acquired from four different devices: Biometrika, Crossmatch, Italdata and Swipe. More than 4000 images were taken with each of the aforementioned devices.

The following materials were used in order to build the fake part of the database: Body Double, Latex, Play-Doh, Wood Glue, Gelatin, Silicon and Modasil. The fake images come from approximately 100 fingers of 20 people for the Crossmatch and Swipe datasets and from 100 fingers of 15 people for the Biometrika and Italdata datasets. Also, for the Crossmatch and Swipe datasets, cooperative methods were used and for the other two, the fingerprints were acquired through non-cooperative ways.

The living images come from 440 fingers of 44 people for the Crossmatch dataset, from 250 fingers of 50 subjects for Swipe and from 300 fingers of 30 subjects for Biometrika and Italdata datasets.

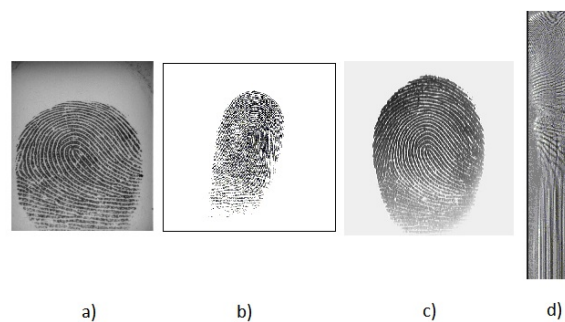


Figure 3.37: Examples of live fingerprints from the LivDet2013 datasets: a) Biometrika, b)Crossmatch, c)Italdata and d) Swipe.



Figure 3.38: Examples of fake fingerprints from the LivDet2013 datasets, using different materials a)Gelatin, b)Latex, c)Play-Doh, d)Body Double and e) Wood Glue.

ATVS database

The ATVS [80] database contains over 3000 live and spoof fingerprint images. The fake fingers were created using silicon and two methods were followed: with and without cooperation.

Three devices were used to acquire the images: the flat optical sensor Biometrika FX2000, the flat capacitive sensor Precise SC100 and the thermal sweeping sensor Yubee with Atmel's Fingerchip.

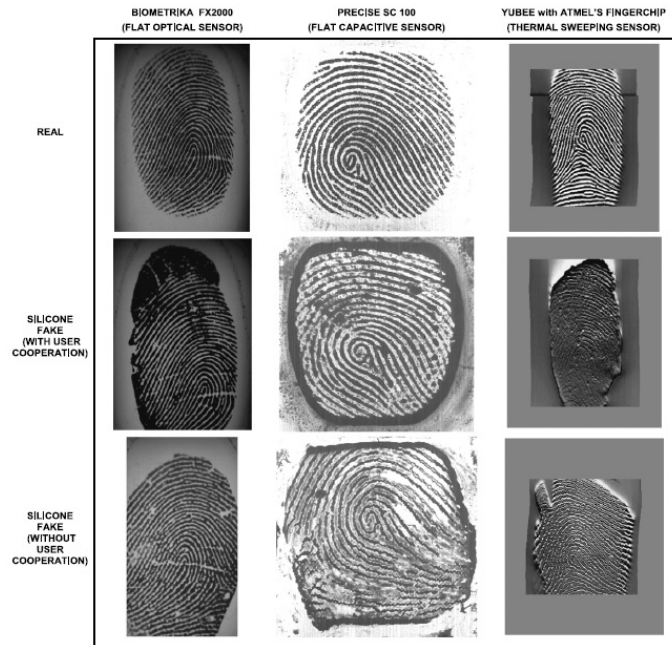


Figure 3.39: Examples of live and fake fingerprints from the ATVS database [79].

3.3 Summary

As can be read in this chapter, plenty of work has been done in the field of Iris and Fingerprint Recognition Systems. However, most of the work requires very constrained conditions and a system with such high accuracy rates that it can be considered completely spoof resistant has not yet been found .

Besides that, liveness detection algorithms may increase the processing time of the global system and usually need the cooperation of the user, particularly if they are hardware-based in which the users are asked for example to blink. Building a robust classifier is also a really important task since, in the situation of a fake sample being classified as a real one, someone unwanted could have access to sensitive data.

We intend to compare liveness detection methods in iris and fingerprint images and see how well they perform. In these traits the texture is a component with high relevance, therefore we use methods that describe this property. The algorithms were chosen based on the results obtained in

previous studies and we intend to analyze if they perform just as well in other databases.

Chapter 4

Methodology

This chapter presents the methodology adopted during the realization of this MSc Dissertation. Two state of the art liveness detection algorithms were selected, aiming to replicate them and test them both in iris and fingerprint databases.

The databases used were the Clarkson [49] and Notre Dame [50] for the iris images, since these possess fake images of irises wearing cosmetic contact lenses.

On the other hand, to test the algorithms in fingerprint images, the four datasets from the LivDet2013 [81] competition were used. More detail about these databases can be found in Sections 3.1.5.3 and 3.2.5.3.

4.1 Segmentation

In order to test the liveness detection algorithms with the iris images, segmentation had to be done since it largely influences the results of the algorithms. That occurs because there is a lot of useless information around the iris that is not needed while performing liveness detection tests. However, there are some methods available capable of working with the whole image too.

Segmentation is thus used to determine the region of interest of the image. We decided to use manual segmentation considering that this task was not one of the goals of this dissertation and we could use the manual segmentation done in the scope of a previous work of the VCMi group [26] that guarantees a reasonable precision.

To do the manual segmentation, three points (the center of the eye, the pupil's border and the iris' border) were marked in every image (Figure 4.1). With those points as a reference, it was possible to consider the contours of the iris as two concentric circumferences.

For the fingerprints, no segmentation was needed and the whole images were used.

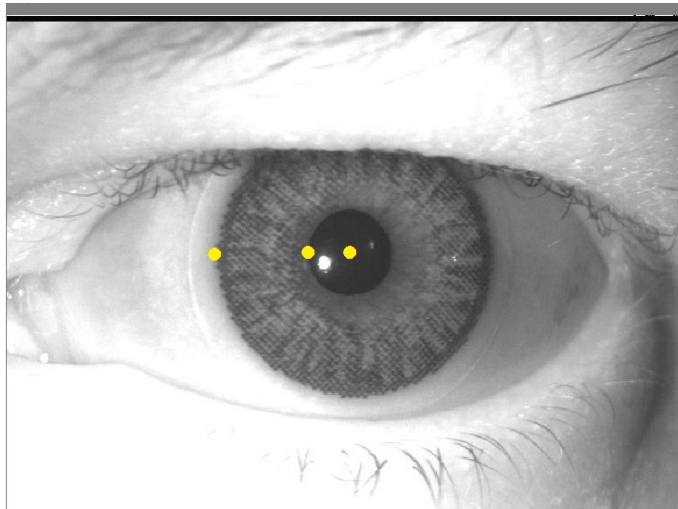


Figure 4.1: Reference points obtained with the manual segmentation.(Example with image from Notre Dame database)

4.2 Algorithms

4.2.1 Algorithm I - Weighted Local Binary Patterns

The first algorithm combines Local Binary Patterns with a Scale Invariant Feature Transform (SIFT) descriptor [82] in order to obtain statistical features capable of describing textural characteristics of images.

Since it is a textural method and both irises and fingerprints are rich in terms of texture, we figured it could be used in both traits.

This method was already tested in iris databases [83], but not the ones used in this dissertation. Also, studies about fingerprint liveness detection using LBP maps do exist [73], but it has not been tested, to our knowledge, this improved version of it.

As we intended to replicate the algorithm specified in [83], we started by segmenting the region of the iris, obtaining a bounding box around it, considered as the region of interest (ROI) of the image. Then, the images were normalized into the same size, 400×400 pixels.

The following step was to create a simplified SIFT descriptor. A SIFT [82] transforms an image into a set of local feature vectors, each of which is invariant to translation, scaling and rotation.

This process starts with the generation of a Gaussian scale space. The output of this operation is a smoothed image in six scales (Figure 4.2).

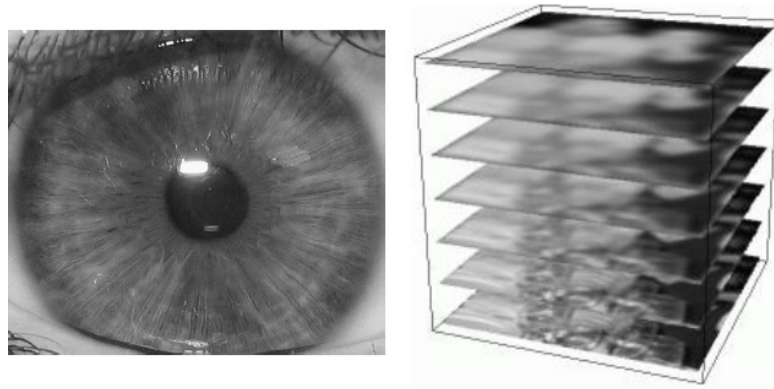


Figure 4.2: Representation of the Gaussian scale space generation (Adapted from [84]).

For each scale, the gradient orientation of each pixel is calculated and, by analyzing every pixel's 5×5 neighborhood, an histogram of gradient orientations is created. A Gaussian window is applied to the neighborhood so that the closest neighbors to the pixel are more relevant than the farthest ones.

Figure 4.3 represents the aforementioned operation. The arrows represent the gradient orientations, the circle is the Gaussian window and the illustration on the right symbolizes an histogram of gradient orientations. The gradient orientations are rotated to the following eight orientations:

$$O = \{0^\circ, 45^\circ, 90^\circ, 135^\circ, 180^\circ, 225^\circ, 270^\circ, 315^\circ\} \quad (4.1)$$

Every histogram is then converted into a descending rank, from 7 to 0. The orientation correspondent to the biggest histogram bin is set to 7 while the lowest is set to 0, as can be seen in the example of Figure 4.5.

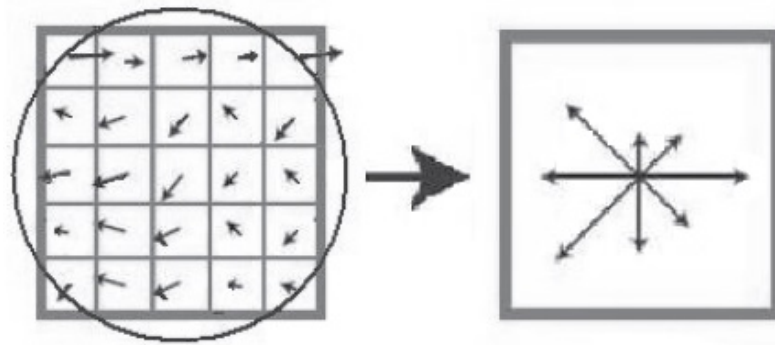


Figure 4.3: Gradient orientations & Histogram of orientations [83].

Since irises have very fine textures that could influence the accuracy of this method, applying a SIFT descriptor to the LBP approach will improve its invariability to local rotations and distortions.

A Local Binary Pattern (LBP) labels the pixels of an image by comparing the neighborhood of

each pixel with the center one. If the neighbor is larger than the center, it is set to one, otherwise it is set to 0. The result is then turned into a binary string (Figure 4.4).

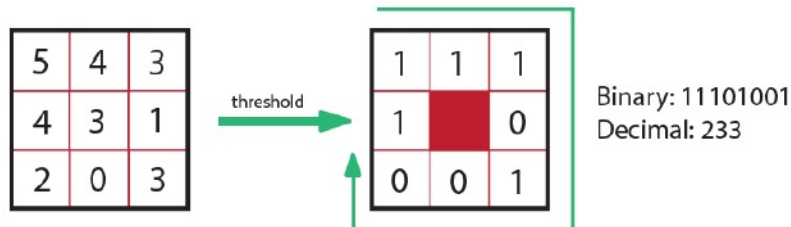


Figure 4.4: Local Binary Pattern method scheme (Adapted from [85]).

One could say that the SIFT descriptor “weights” the LBP by combining the descending SIFT rank with the LBP neighborhood map. This process can be better understood by observing Figure 4.5. Basically, for each of the 8 positions (excluding the central one) of the 3×3 matrix, the binary LBP response should be placed in the binary string considering the position given by the SIFT rank number.

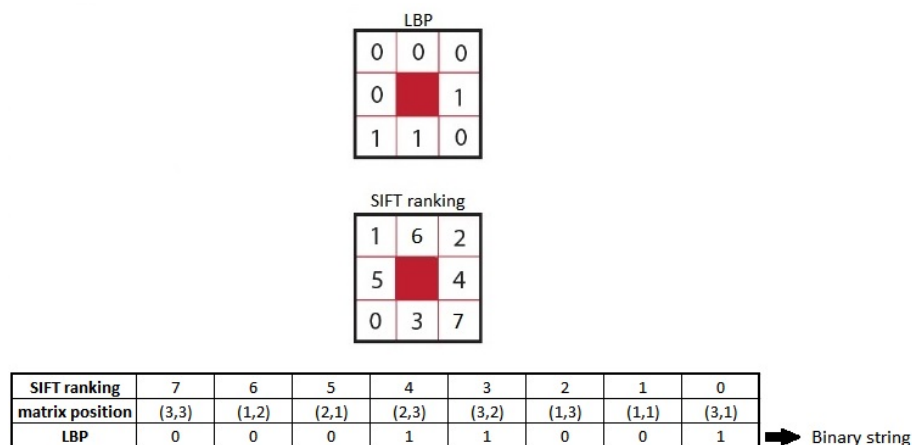


Figure 4.5: Weighted LBP process

The binary string is then converted to decimal thus obtaining a decimal number for each pixel of the image. We call that a weighted LBP map.

Although we obtain six scales when the Gaussian scale space function is applied, we will only get four weighted LBP maps. That occurs because we obtain the regular weighted LBP map for the three first SIFT scales, but we combine the last three scales by comparing their neighborhood pixels when computing the LBP for each pixel (Figure 4.6). In this case, we set a neighbor to 1 only if at least two out of three neighbors are larger than the center pixel. We are then comparing, at this phase, 24 neighbors with the center pixel, instead of only eight [83].

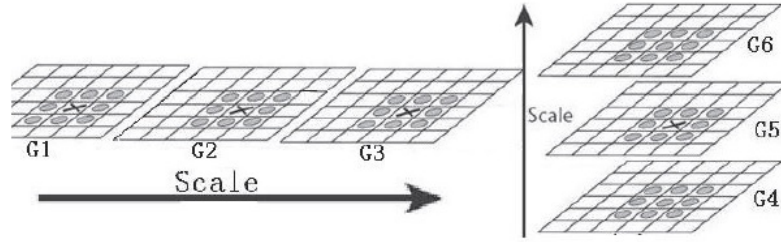


Figure 4.6: Weighted LBP at different scales [83].

At this point, we want to extract statistical features out of the weighted LBP maps. We divide each weighted LBP map in 8×8 blocks and discard the first and last lines of blocks to avoid obstructions from eyelids and eyelashes, obtaining a map of 300×400 pixels.

For each block, three statistical features are extracted: the standard deviation of weighted LBP histogram, the mean of the weighted LBP map and the standard deviation of the weighted LBP map. That results in a 576 dimensional feature (300×400 pixels \times 4 weighted LBP maps \times 3 statistical features) for each image.

4.2.2 Algorithm II - Gray Level Co-occurrence Matrices

This method is based on Gray Level Co-occurrence Matrices (GLCM) and its use for liveness detection has been described in several previous works [41, 86, 87, 48].

Based on the state of the art article used as a reference to replicate this method [41], iris images are normalized using bilinear interpolation in order to project iris from Cartesian to Polar coordinates (Figure 4.7 c)). However, since the most useful iris information used to detect contact lenses distributes in the outer portion of the contact lens and the lower part of it usually has less obstructions, only the lower half part of the iris image is used.

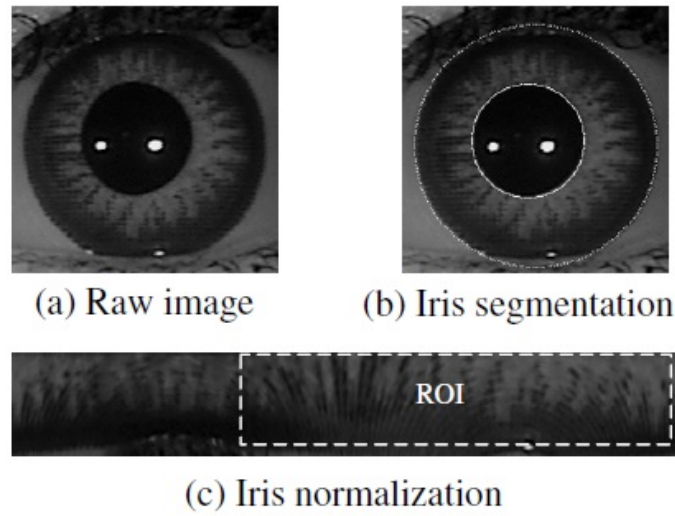


Figure 4.7: GLCM method - Iris image pre-processing [41].

Co-occurrence matrices characterize the relationship between neighboring pixels (Figure 4.8). Each element $p(i, j)$ of a GLCM matrix represents the relative frequency with which two neighboring pixels separated by a certain distance occur, one with a gray scale i and another with a gray scale j [48].

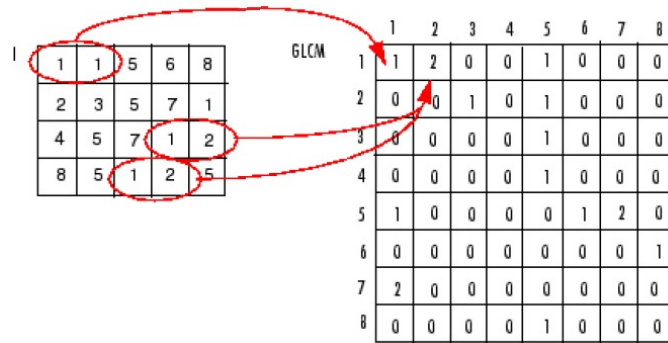


Figure 4.8: Example of the creation of a GLCM matrix [26].

Haralick et al. [86] define 14 features that can be extracted from a GLCM matrix, these are:

1) Angular Second Moment (ASM):

$$f_1 = \sum_i \sum_j \{p(i, j)\}^2 \quad (4.2)$$

where $p(i, j)$ is the (i, j) th entry in a normalized gray-tone spacial-dependence matrix.

2) Contrast:

$$f_2 = \sum_{n=0}^{N_g-1} n^2 \left\{ \sum_{i=1}^{N_g} \sum_{\substack{j=1 \\ |i-j|=n}}^{N_g} p(i, j) \right\} \quad (4.3)$$

where N_g is the number of distinct gray levels in the quantized image.

3) Correlation:

$$f_3 = \frac{\sum_i \sum_j (i, j) p(i, j) - \mu_x \mu_y}{\sigma_x \sigma_y} \quad (4.4)$$

4) Sum of Squares (Variance):

$$f_4 = \sum_i \sum_j (i - \mu)^2 p(i, j) \quad (4.5)$$

5) Inverse Difference Moment:

$$f_5 = \sum_i \sum_j \frac{1}{1 + (i - j)^2} p(i, j) \quad (4.6)$$

6) Sum Average:

$$f_6 = \sum_{i=2}^{2N_g} i p_{x+y}(i) \quad (4.7)$$

7) Sum Variance:

$$f_7 = \sum_{i=2}^{2N_g} (i - f_6)^2 p_{x+y}(i) \quad (4.8)$$

8) Sum Entropy:

$$f_8 = - \sum_{i=2}^{2N_g} p_{x+y}(i) \log \{ p_{x+y}(i) \} \quad (4.9)$$

9) Entropy:

$$f_9 = - \sum_i \sum_j p(i, j) \log(p(i, j)) \quad (4.10)$$

10) Difference Variance:

$$f_{10} = \text{variance of } p_{x-y} \quad (4.11)$$

11) Difference Entropy:

$$f_{11} = - \sum_{i=0}^{N_g-1} p_{x-y}(i) \log \{ p_{x-y}(i) \} \quad (4.12)$$

12) & 13) Information Measures of Correlation:

$$f_{12} = \frac{HXY - HXY1}{\max(HX, HY)} \quad (4.13)$$

$$f_{13} = (1 - \exp[-2.0(HXY2 - HXY)])^{\frac{1}{2}} \quad (4.14)$$

$$HXY = - \sum_i \sum_j p(i, j) \log(p(i, j)) \quad (4.15)$$

where HX and HY are entropies of p_x and p_y , and

$$HXY1 = - \sum_i \sum_j p(i, j) \log\{p_x(i)p_y(j)\} \quad (4.16)$$

where $p_x(i)$ and $p_y(j)$ are the i th entry in the marginal-probability matrix, obtained by summing the rows/columns of $p(i, j)$.

$$HXY2 = - \sum_i \sum_j p_x(i)p_y(j) \log\{p_x(i)p_y(j)\} \quad (4.17)$$

14) Maximal Correlation Coefficient:

$$f_{14} = (\text{second largest eigenvalue of } Q)^{\frac{1}{2}} \quad (4.18)$$

where

$$Q(i, j) = \sum_k \frac{p(i, k)p(j, k)}{p_x(i)p_y(k)} \quad (4.19)$$

These features are orientation dependent so four values can be obtained for each feature based on the four orientations (0°, 45°, 90°, 135°)(Figure 4.9).

The mean and standard deviation of the four values (four orientations) of each 14 measures, compose a set of 28 features.

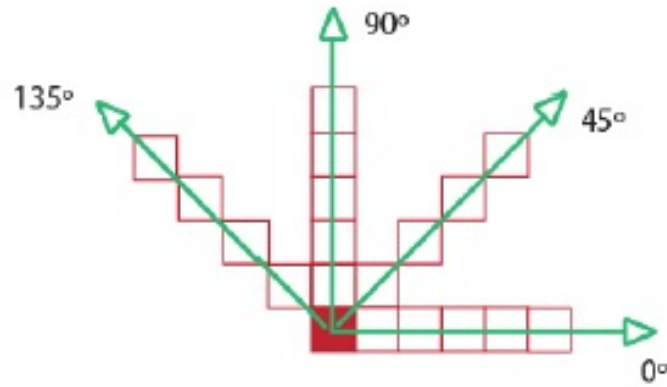


Figure 4.9: Directions used for the GLCM calculations (Adapted from [85]).

4.3 Classification

Classification is a critical task in liveness detection. Its objective is to categorize one or more classes by labeling each similar set of data as one class. In the specific case of liveness detection, it can be seen as a two class classification problem, in which we intend to label each sample as fake or real.

A regular classifier is constructed in two phases: the training and the testing. In the first phase, a training set is used to decide how the features should be weighted in order to separate the different classes. During testing, the weights selected in the training set are applied to another set of data, outputting the class that they should belong to [88].

Previous results [26] show, by comparing several classifiers such as k-Nearest Neighbor, Discriminant Analysis and Support Vector Machines, that this last one performs better than the others in liveness detection situations and thus we decided to use it in the work. Support Vector Machines (SVM) are based on the concept of decision planes. A decision plane splits a set of objects having different classes thus defining the boundary between one class and another.

There are two main types of SVM classification methods, a binary and a multi-class. It also supports two tasks, regression and classification, being also efficient when working with large-scale samples and variables.

Since we are dealing with the problem “Is this image real or false?” we are using a binary SVM classifier with linear kernel, taking advantage of the LIBSVM package [89] for Matlab.

Chapter 5

Experimental Setup and Results

This chapter presents the results obtained by applying the methodology described in Chapter 4 for liveness detection in iris and fingerprint recognition systems. A brief explanation of what actions were performed is also present, as well as some global information about the databases chosen.

5.1 Databases

5.1.1 Iris

The databases selected to test the liveness detection methods in iris images were the Clarkson and Notre Dame databases. This choice was made because these are the only databases, to our knowledge, with fake samples using cosmetic contact lenses.

More information about this database can be found in Section 3.1.5.3.

5.1.2 Fingerprint

To test the algorithms in fingerprint images, the four datasets from the LivDet2013 [81] were used. The four datasets correspond to four sensors used to collect the images. It is also a very diverse database since several types of materials were used to create the dummy fingers: gelatin, latex, ecoflex, wood glue, Play-Doh, etc.

More information about this database can be found in Section 3.2.5.3.

5.2 Feature Extraction

5.2.1 Weighted Local Binary Patterns

For the wLBP method we started by obtaining the weighted LBP maps for both fake and real images of the Clarkson [49] and Notre Dame [50] databases. As quoted before, the fake samples of these databases are from iris using cosmetic contact lenses.

Since we are working with 3 simple scales plus a combined one (scale 4, 5 and 6), we obtained a

$300 \times 400 \times 4$ map for each image.

From these maps, 3 statistical features were extracted: the standard deviation of weighted LBP histogram, the mean of the weighted LBP map and standard deviation of weighted LBP map, obtaining thus a 576 dimensional feature for each image.

The procedure for this method using Fingerprint Datasets was similar to the one explained above. The main difference between these implementations is that, for the fingerprint images, no segmentation was needed and the whole images were used.

5.2.2 Gray-Level Co-Occurrence Matrices

For this method we started by obtaining a GLCM matrix for every picture, using four orientations: 0° , 45° , 90° , 135° . Even though fourteen measures are detailed in Section 4.2.2, 13 features were extracted from these matrices, that is, 13 measures for each of the four orientations. The last measure was not extracted due to computational instability.

We then obtained the mean and standard deviation of those 4 values of each measure thus getting 26 features, that were then used by the classifier.

Similarly to what has been stated for the first method, this second method has similar procedures for both iris and fingerprint images. However, there is no need to normalize the fingerprint and so, the whole images were used in that case.

5.3 Learning methodology

5.3.1 Feature Selection

Due to the large dimensionality of features, it is possible that the best classification results are obtained not by using them all, but using a subset of features. Testing all the possibilities to determine the best subset of features is impracticable, so a feature selection method was used to investigate whether it is possible to reduce the error rate of a method by using less features.

The method chosen was the Minimum Redundancy - Maximum Relevance (mRMR) [90]. This is a model-independent criteria (filter method) that provides a ranking of the features. Its approach is based on mutual information, that is, the amount of information shared by different features [91]. It selects a subset of features that are maximally dissimilar to each other or their correlations are minimized.

5.3.2 Classification results using SVM

SVM was the classifier chosen for this work as it has presented better results in liveness detection situations in previous studies.

We run the SVM classifier 50 times using a polynomial kernel. For each of the 50 cycles, a “grid-search” was performed on the parameters of the models. The exponential growth of $C = 2^N$ was tested, with N varying from -1 to 15 . The polynomial degree (d) was tested with the following values $\{1, 2, 3, 4, 5\}$. We used this technique to obtain the best parameters (d, C) to use for the estimation of the testing set classes.

In each run, the results were obtained by dividing randomly 62.5% of the samples for training and 37.5% for testing.

5.3.3 Cross-Validation

Cross-validation is a technique to estimate the performance of a predictive model and it gives an indication of how well the learner will perform when it is asked to predict the class of new data that has not been already used.

The holdout method, also called 2-fold cross-validation, was the method chosen for this work. In this method, the data set is split into two sets, the training set and the testing set. A function that fits the training data is found by a function approximator and then that function is used to predict the output values for the testing set [92]. However, this evaluation may depend on which data end up in the training set and which end up in the testing set.

The function used in this dissertation returns logical index vectors for cross-validation of N observations. That is done by randomly selecting the percentage of data tested times N (approximately) observations to hold out for the evaluation set.

5.4 Evaluation Metrics

To evaluate the accuracy of the classification method used, the misclassification rate of each of the 50 iterations was calculated as:

$$\text{misclassificationRate} = \frac{\sum(\text{predicted data class} \neq \text{true data class})}{\text{length of data}} \quad (5.1)$$

The mean and standard deviation of the misclassification rates allow us to analyze the overall performance of the classification.

5.5 Results for the Iris images

Table 5.1 presents the results obtained using Iris databases for both studied algorithms. The results are expressed as the percentage (%) of classification error. The columns “mean” correspond to the mean classification error and σ stands for standard deviation.

For Algorithm I, we also used an available LBP algorithm [93] in order to compare results. We tested this method using 8 and 16 neighbors, using the histogram of the obtained maps, since it is

considered to be a powerful textural feature.

In this table, LBP_8 stands for the available LBP algorithm [93] using 8 neighbors of each pixel, LBP_{16} stands for the LBP algorithm using 16 neighbors and wLBP corresponds to the implemented weighted LBP method (see Section 5.2.1).

For the GLCM method, $GLCM_1$ corresponds to the results obtained using the algorithm reported in [26] and $GLCM_2$ refers to the use of the Matlab functions available, *graycoprops*. Finally, $GLCM_3$ corresponds to the method described in the previous chapter (Section 5.2.2).

	Notre Dame		Clarkson	
	mean	σ	mean	σ
LBP_8	1.95	0.35	17.62	2.00
LBP_{16}	0.79	0.28	15.11	1.84
wLBP	0.52	0.21	17.43	2.47
$GLCM_1$	13.92	1.20	26.77	2.32
$GLCM_2$	36.40	0.99	36.69	2.25
$GLCM_3$	2.59	0.63	3.60	0.47

Table 5.1: Results of the SVM Classifier for GLCM and weighted LBP Features using Iris images

In Table 5.1 it is noticeable that the overall best result was obtained by the weighted LBP method, using the Notre Dame database, resulting in a final mean error rate of 0.52%. The improved version of the LBP method resulted in lower classification errors for the Notre Dame database, nevertheless, for the Clarkson database, the wLBP result is comparable with the simple LBP, using 8 neighbors and, in this case, the best performance outcomes from the application of the simple LBP, using 16 neighbors, leading to a error of 15.11%.

The GLCM method resulted in lower classification errors for the Notre Dame and Clarkson database than for the State of the Art approaches. The fact that the results were much better using 26 features, in both databases, shows that using only 8 features, as happens in $GLCM_1$ and $GLCM_2$, is not enough.

The difference of computation time of the methods using local binary patterns is quite large, since it takes 2 seconds to obtain the features of each image with the simple LBP method, while with the weighted LBP it takes around 147 seconds (2.45 minutes). This time difference is not significant for the GLCM approaches, as the method extracting more features, $GLCM_3$, only takes approximately 3 seconds for each image.

The distinctness of results from one database to another could be related to the quality of the images, being this difference more significant for the LBP methods than for the GLCM ones.

Also, the differences between the 14 types of contact lenses present in the Clarkson database, could also lead to higher error rates since the images are not as similar as the ones from Notre Dame. That is also noticeable by examining the standard deviations for this database, that are substantially bigger.

5.6 Results for the Fingerprint images

The following tables (Table 5.2, Table 5.3, Table 5.4 and Table 5.5) present the results obtained for the fingerprint images. Each table corresponds to one of the datasets from the LivDet competition thus to one of the sensors used to capture the images: Biometrika, CrossMatch, Italdata and Swipe. In these tables, only the results for the methods described in Chapter 4 are presented.

	Biometrika									
	Ecoflex		Gelatin		Latex		Modasil		Wood Glue	
	mean	σ	mean	σ	mean	σ	mean	σ	mean	σ
wLBP	0.78	0.22	3.82	0.61	1.54	0.40	0.98	0.38	1.38	0.38
GLCM ₃	16.97	1.01	16.65	1.03	16.62	1.04	16.32	0.79	16.66	1.16

Table 5.2: Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - Biometrika dataset.

Table 5.2 shows that the weighted LBP method performs better than the GLCM method using the Biometrika dataset. For the weighted LBP, the best outcome is the one resulting from the use of Ecoflex fake samples: 0.78% of mean error. For the GLCM method, the results are weighted in the range of]16, 17[, corresponding the best one to the Modasil fingerprints: 16.32% of error. The high GLCM method error rates may have to do with the “curse of dimensionality”. That is, using all features could not be resulting in the best outcome and a subset of these features could result in lower classification errors. This means that, in this case, performing feature selection could be necessary. A test using feature selection is presented in Section 5.7.

	CrossMatch							
	Body Double		Latex		Play-Doh		Wood Glue	
	mean	σ	mean	σ	mean	σ	mean	σ
wLBP	16.63	0.75	16.54	0.96	16.58	0.93	16.63	0.76
GLCM ₃	16.57	0.91	16.54	0.85	16.57	0.86	16.69	0.86

Table 5.3: Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - CrossMatch dataset.

The results for CrossMatch dataset, presented in Table 5.3, were unexpected, especially for the weighted LBP method, that shows higher results than the ones got for the other datasets. The best results for both method were approximately the same, 16.54%, for the Latex fake dummies images. However, the standard deviation for these images was slightly higher for the weighted LBP method.

The range of values for the GLCM method remains the same obtained for the previous dataset, confirming that feature selection should be employed in order to get a subset of features that lower the error rate obtained. As quoted before, a test using a feature selection method was performed

and the results can be seen in Section 5.7.

	Italdata									
	Ecoflex		Gelatin		Latex		Modasil		Wood Glue	
	mean	σ	mean	σ	mean	σ	mean	σ	mean	σ
wLBP	1.13	0.30	1.36	0.41	1.42	0.38	0.82	0.31	1.22	0.48
$GLCM_3$	16.61	1.11	16.56	0.99	16.40	0.79	16.79	0.75	16.82	0.95

Table 5.4: Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - Italdata dataset

The results for the Italdata dataset, presented in Table 5.4, are comparable to the ones obtained with Biometrika dataset (Table 5.2). Likewise, we obtained better results for the weighted LBP method, while for the GLCM method the results are around 16.5%.

In this case, the best result for the weighted LBP method is the one got with Modasil images and, for the GLCM, the best result is the Latex images classification error outcome.

	Swipe							
	Body Double		Latex		Play-Doh		Wood Glue	
	mean	σ	mean	σ	mean	σ	mean	σ
wLBP	6.93	0.78	8.78	0.93	5.51	0.92	5.23	0.68
$GLCM_3$	1.60	0.49	5.86	0.61	9.34	1.00	13.57	1.12

Table 5.5: Results of the SVM Classifier for GLCM and weighted LBP Features using the LivDet2013 - Swipe dataset

The results obtained using the Swipe sensor (Table 5.5) are a little bit higher, for the weighted LBP method, than the ones obtained for the rest of the datasets, except CrossMatch, but unexpectedly lower for the GLCM method.

The best result for the wLBP method was obtained with the Latex dummies, and for the GLCM, with the Body Double fake samples.

5.6.0.1 Types of fake fingerprints comparison

In Table 5.6, a comparison between types of fake fingerprint dummies is presented, where it can be observed which type of mold and sensor results in better classification results.

Type	wLBP	Dataset	GLCM	Dataset
Ecoflex	0.78	Biometrika	16.61	Italdata
Gelatin	1.36	Italdata	16.56	Italdata
Latex	1.42	Italdata	5.86	Swipe
Modasil	0.82	Italdata	16.32	Biometrika
WoodGlue	1.22	Italdata	13.57	Swipe
Body Double	6.93	Swipe	1.60	Swipe
Play-Doh	5.51	Swipe	9.35	Swipe

Table 5.6: Best results for the each type of fake mold.

The previous table shows that Italdata and Swipe are the sensors that present better results for both methods. It is also observable that there is quite a difference between the wLBP results and the GLCM ones, showing that the first method has a better performance than the second. However, as quoted before, the high results for the GLCM method could be lower, if feature selection was applied to all datasets.

Body Double contradicts the overall results, as it presents better results for the GLCM method than for the wLBP, being the results obtained, in both cases, using the Swipe sensor images.

5.7 Feature Selection Test

As the error rates for the GLCM methods in fingerprint images were overall higher than the ones obtained for the weighted LBP method, we decided to apply a simple filter feature selection method, to reduce the number of features used. As mentioned before, the method chosen was the mRMR (minimum redundancy - maximum relevance) and it was tested only with the most challenging dataset, CrossMatch.

In order to do that, the data was divided in *training* and *testing* sets, the feature selection method was applied to the *training* set and for each cardinality, that is, for each subset of features chosen, the classification parameters were optimized, the model was trained and it was then tested in the *testing* set. The results obtained for each cardinality can be found in the Appendix, in Section 7.3. Table 5.7 presents the best results obtained with and without feature selection. In that table, # stands for the number of features used to classify the images.

	CrossMatch							
	BodyDouble		Latex		Play-Doh		WoodGlue	
	#	mean	#	mean	#	mean	#	mean
GLCM	26	16.57	26	16.54	26	16.57	26	16.69
GLCM + FS	10	6.31	15	7.22	11	8.15	15	12.03

Table 5.7: Features selection results for the Crossmatch dataset with the GLCM method.

By observing the results obtained using a feature selection method we can see that it has reduced the error rate for the CrossMatch dataset, by using approximately half of the features used in the

previous tests. The best result obtained using the feature selection method is 6.31%, for the Body Double mold, compared to the 16.57% obtained without feature selection.

Besides lowering the error rates, by using less features, the classification process becomes less time consuming.

However, it could be possible to get even better results by searching a more elaborate feature selection technique, like a wrapper method.

5.8 Comparative analysis with State of the Art

5.8.1 Comparison of methods' results in different databases

The following charts (Figure 5.1 and Figure 5.2) present the best results for each database using the weighted LBP and GLCM methods. The results obtained by the authors of these methods are also presented. Zhang et al. [83] tested their algorithm using a self collected fake iris database and another database stated just as DB5. The real images come from CASIA and a new iris database that is not specified in the article. Experiments were performed on each database separately, using half of the images for training and the rest for testing (corresponding to the first bar of Figure 5.1) and then the databases were mixed and one fourth of the images were used for training and the rest for testing (second bar of Figure 5.1).

On the other hand, Wei et al. [41] fake databases are also self collected, corresponding to two cosmetic contact lenses manufacturers, and the real images come from the CASIA and BATH databases. The first bar of Figure 5.2 corresponds to the test made using one type of cosmetic contact lenses and the second using another.

State of the art results are presented in black, iris results are shown in dark grey and fingerprint results are displayed in light grey.

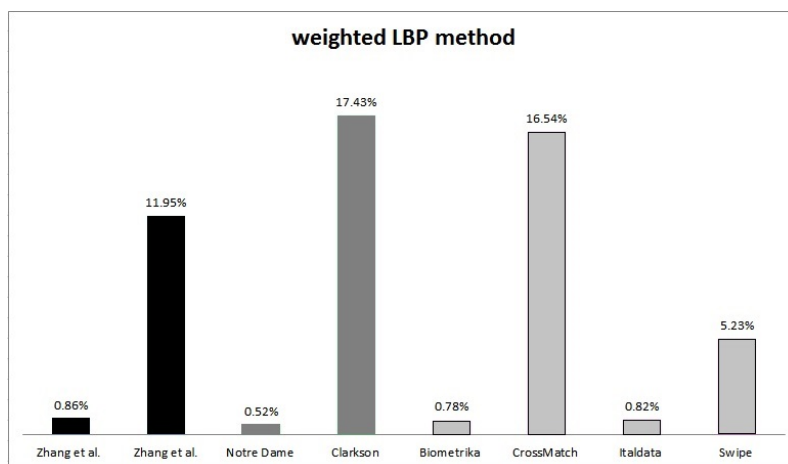


Figure 5.1: Classification Errors for the wLBP method.

Observing Figure 5.1 we can conclude that this method does not perform linearly for all databases. For the iris images, only with the Notre Dame database was possible to obtain comparable or slightly better results than the state of the art. For the fingerprint images, only CrossMatch dataset performed worse than expected. However, Swipe results are still a bit worse than the remaining.

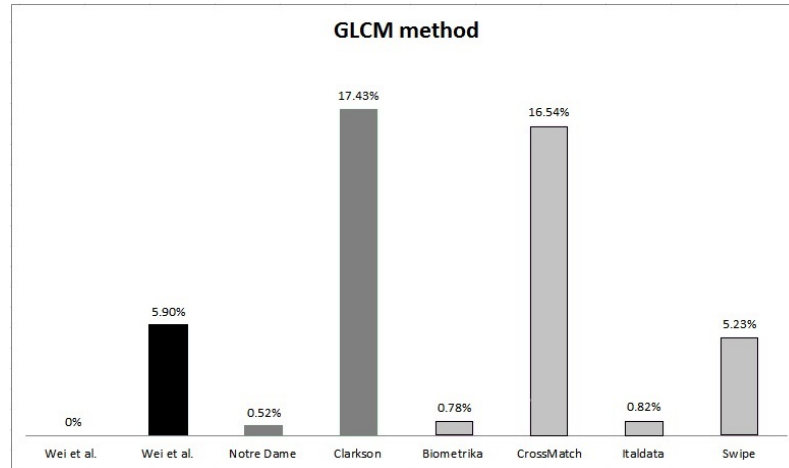


Figure 5.2: Classification Errors for the GLCM method.

For the GLCM method, similar results were obtained. For iris images, the Clarkson database presents worse results than expected, reinforcing that feature selection should be implemented and for fingerprint images, CrossMatch also performed below average.

Comparing the results of both methods we could say that both Clarkson and Crossmatch are the most challenging databases.

5.8.2 Comparison of different methods' results using the Notre Dame, Clarkson and LivDet2013 databases

In this section we present a series of charts representing the classification results, in terms of error, for the Clarkson, Notre Dame and LivDet2013 databases. These graphs compare the performance of different methods in the same databases. With this section we aim to analyze whether the chosen methods are superior in terms of accuracy relatively to other methods available. The graphs can be better observed in the Appendix, in Section 7.1 and 7.2.

Iris images databases are compared with the results obtained in the LivDet2013 Iris competition [94] which had three submissions: from the Biometric Recognition Group of Universidad Autonoma de Madrid (ATVS), from the University of Naples Federico II (Federico) and from the Engineering Faculty of Oporto University - FEUP (Porto). Only the Federico participants submitted results for the Notre Dame database so we can only compare the results from this dissertation with those.

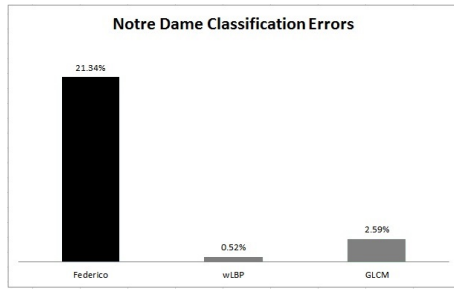


Figure 5.3: Classification Errors for the Notre Dame database

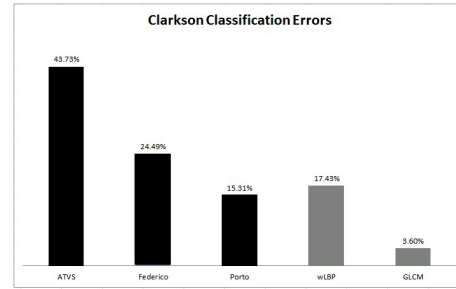


Figure 5.4: Classification Errors for the Clarkson database.

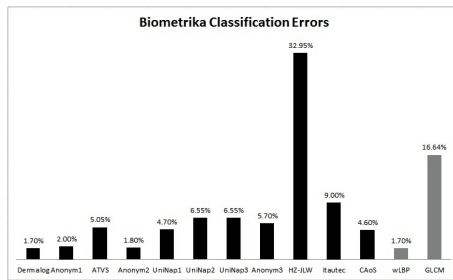
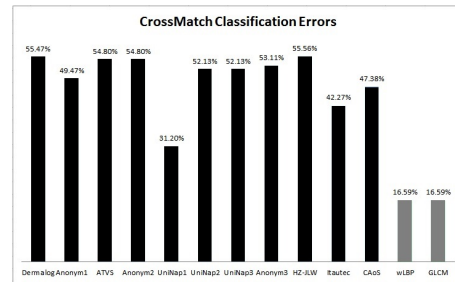
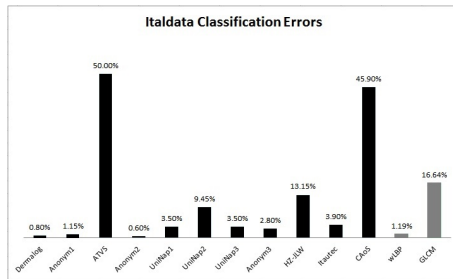
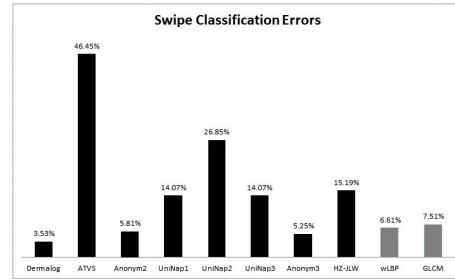
Figures 5.3 and 5.4 show that we were able to obtain better results for the Notre Dame database. However, since we were only able to compare the results with one other method, it is not possible to affirm that this is the best method available.

For the Clarkson database, the results are a bit unstable as we were able to get good results with the GLCM method, but the mean errors for the wLBP method are considerably high.

The high errors were expected, as we had already concluded that this is a defiant database and more work should be done in order to lower this high error rates.

The methods used were also compared with state of the art ones for the fingerprint datasets. In this case, we used the results from the LivDet2013 Fingerprint competition [81]. The participants of this competition were:

- Dermalog Identification Systems GmbH (Dermalog);
- First anonymous participant (Anonym1);
- Universidad Autonoma de Madrid (ATVS);
- Second anonymous participant (Anonym2);
- University of Naples Federico II - first algorithm (UniNap1);
- University of Naples Federico II - second algorithm (UniNap2);
- University of Naples Federico II - third algorithm (UniNap3);
- Third anonymous participant (Anonym3);
- HangZhou JLW Technology Co Ltd (HZ-JLW);
- Federal University of Pernambuco (Itaotec);
- Chinese Academy of Sciences (CAoS);

**Figure 5.5:** Biometrika Classification Errors**Figure 5.6:** CrossMatch Classification Errors**Figure 5.7:** Italdata Classification Errors**Figure 5.8:** Swipe Classification Errors

It has been stated before that the results for the GLCM method are generally worse than the wLBP ones. However, considering the results obtained with the Feature Selection Test (Section 5.7), it would be possible to get lower values if feature selection was performed for all databases. For the Biometrika dataset, the best result is comparable to the best method submitted to the competition and the GLCM is the second worst.

CrossMatch is one of the most challenging datasets and thus all the results are significantly bad. However, we were still able to obtain better results than the ones presented in the competition.

The results for the Italdata dataset are quite diversified. Our best result is slightly worse than the best one found in state of the art and, similarly to what happens with Biometrika, the GLCM method is the second worst result.

For the Swipe dataset, our results are neither the best nor the worst, compared to the ones obtained by the participants of the LivDet2013 competition.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

During the research and the development of this work, it was possible to better understand the liveness detection problem and how iris and fingerprint recognition systems work.

Even though the usage of iris and fingerprints in recognition systems is now usual, there is still a need to improve their efficiency, security and applicability.

Detecting the liveness detection of these traits is a great concern as successful spoofing attacks may lead to the leakage of important information or theft of important objects.

In this work we selected and implemented two liveness detection algorithms and tested them in both iris and fingerprint databases aiming to compare their accuracy and relationship between traits.

We worked with two iris databases: *Notre Dame* and *Clarkson* and four datasets from the fingerprint database *LivDet2013*: *Biometrika*, *CrossMatch*, *Italdata*, and *Swipe*. Each of these corresponding to a sensor used to capture the images.

The two iris databases are quite singular as their fake samples correspond to iris wearing cosmetic contact lenses. This fact allowed us to use the same algorithms for both iris and fingerprint, as they both have textural characteristics.

The most important step of this work was feature extraction, as the classification of images depends on the relevance of the extracted features. Two types of texture features were extracted: an improved LBP feature and GLCM features. In the weighted LBP feature, only one feature, with 576 dimensionality, was used for classification. In the GLCM method, 26 features were extracted. In terms of classifier, the SVM was chosen, because it has presented the best results in previous works.

The results show that in general the weighted LBP method performs better than the GLCM. This second method gives promising results for the iris images, but high error rates for the fingerprint images.

For the fingerprint images, it was also shown that the *Italdata*, *Swipe* and *Biometrika* sensors are the ones resulting in a better outcome and the *CrossMatch* is more challenging.

In order to assess if it would be possible to obtain better results, we performed a test consisting in selecting a subset of features that could increase the accuracy of the classification. The test showed that it is possible to improve the results and that the application of a better feature selection method would be relevant.

Comparing the obtained results with the state-of-the-art ones, it has been shown that, even though in some cases it was possible to obtain comparable or even better results, in some datasets, the results were much worse than expected, showing that these methods' results vary from database to database. We may conclude that, although this work has showed that some good classification results are already reachable, the study and the search for a better solution is still needed, as in the security field, the error rate needs to be practically null.

6.2 Future Work

This dissertation intended to compare liveness detection methods for iris and fingerprint images. It was not possible - nor was under the scope of this work - to explore, implement and test all possible methods available. However, some other strategies and paths could be followed in the future. This document ends with suggestions of potential directions and possibilities for future studies about this theme.

First of all, making some improvements to the two algorithms presented could boost their robustness and uniformity to different databases. Searching a more consistent feature selection method and applying it to every database could also help to improve the results obtained.

Testing new methods, combining methods, trying new classifiers or kernel functions for the SVM used, could not only enhance the system performance, but also help to understand whether the options made during this dissertation were the best ones.

Since liveness detection methods usually increase the processing time of the global recognition system, it could be profitable to implement them in more efficient language, such as C++ or Java. Also, the segmentation of iris images should be done automatically as we can not call it an "automatic recognition" if part of the process is done manually.

Lastly, the final suggestion would be to implement the liveness detection algorithms presented in a functional prototype.

Chapter 7

Appendix

7.1 Iris Results Graphs - Comparative analysis with State of the Art

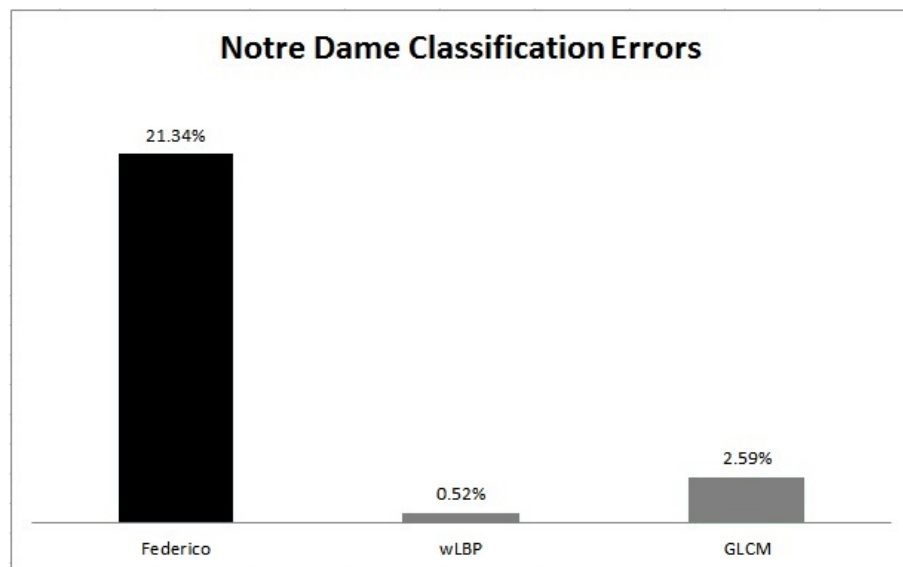


Figure 7.1: Classification Errors for the Notre Dame database

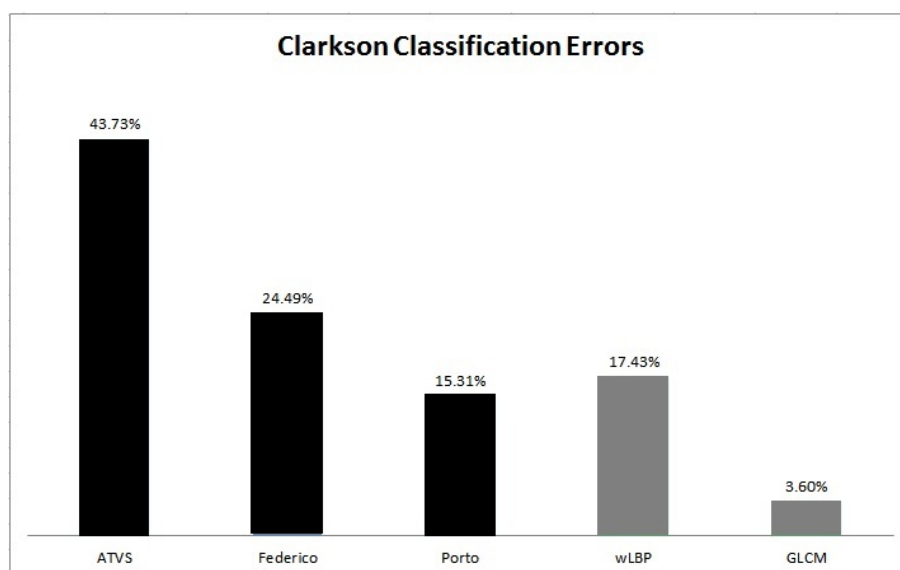


Figure 7.2: Classification Errors for the Clarkson database

7.2 Fingerprint Results Graphs - Comparative analysis with State of the Art

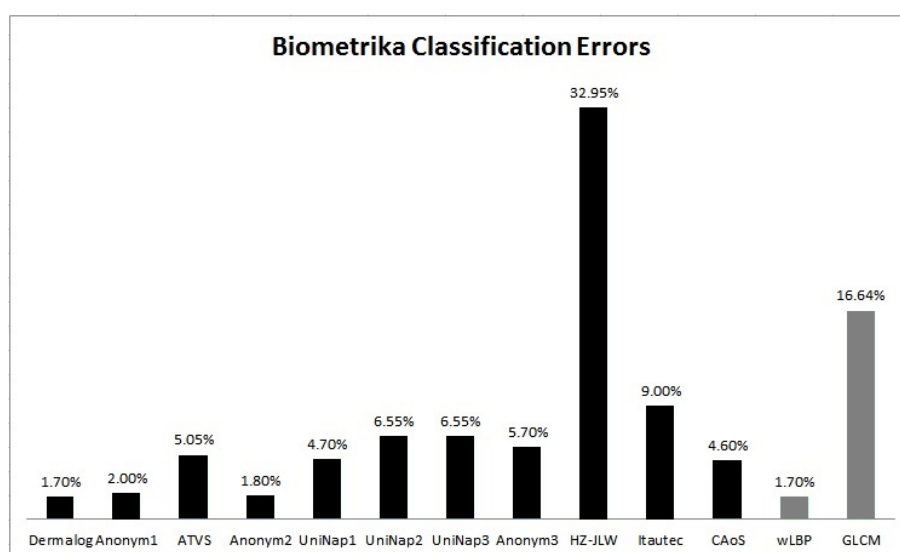
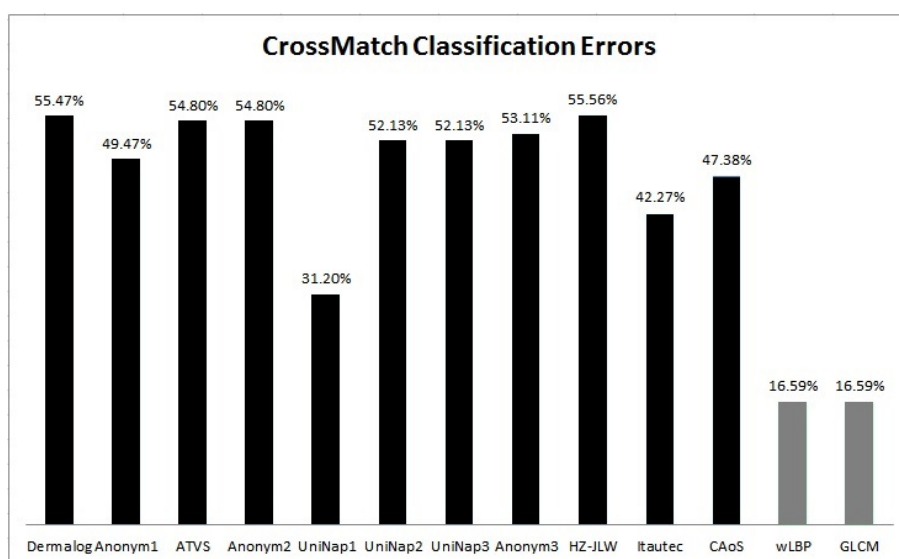
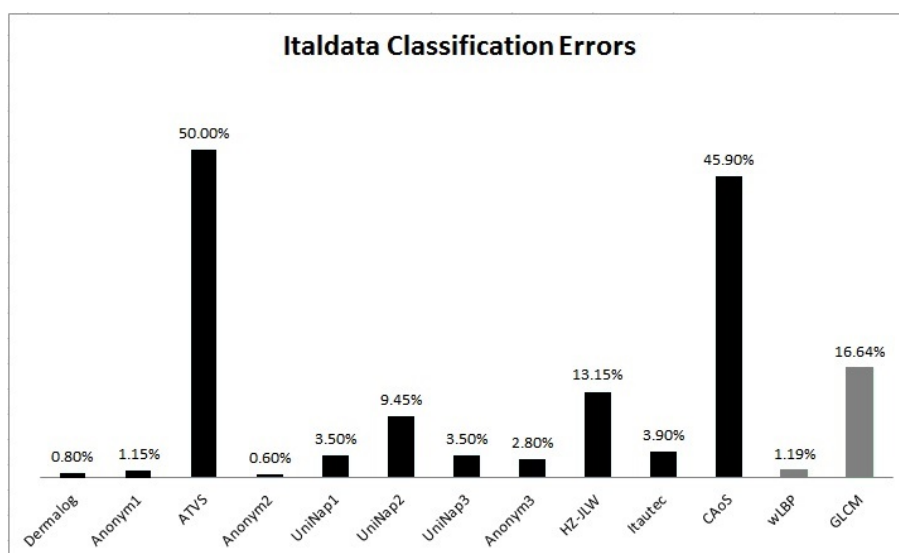


Figure 7.3: Biometrika Classification Errors

**Figure 7.4:** CrossMatch Classification Errors**Figure 7.5:** Italdata Classification Errors

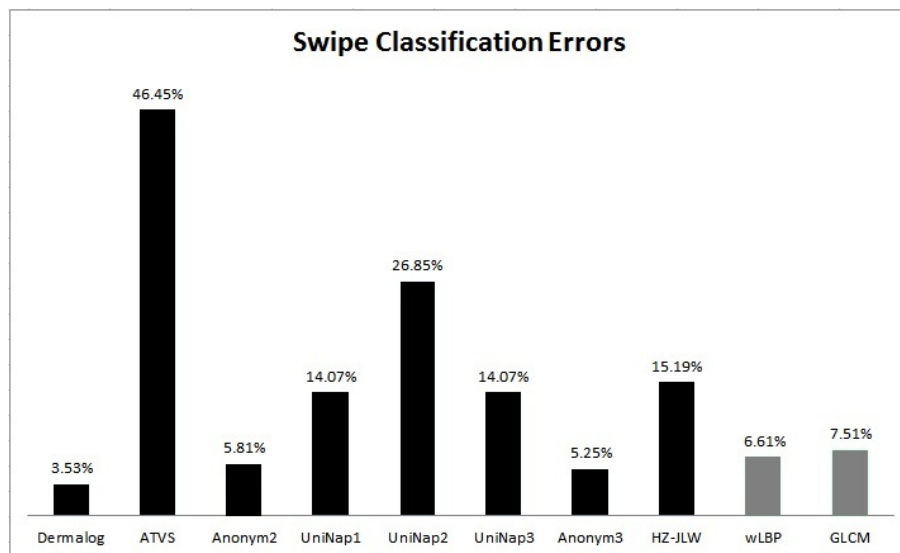


Figure 7.6: Swipe Classification Errors

7.3 Feature Selection Test

Nb. features	CrossMatch			
	Body Double	Latex	Play-Doh	WoodGlue
2	10.36	24.68	8.92	16.09
3	10.54	20.36	8.83	16.71
4	12.62	17.96	9.70	17.42
5	9.36	14.20	12.12	18.04
6	11.72	14.72	13.78	20.62
7	10.24	10.93	10.28	19.20
8	6.41	11.43	9.31	17.60
9	7.04	8.78	9.56	21.51
10	6.31	8.60	8.44	18.65
11	8.36	9.37	8.15	20.54
12	bf 6.88	9.06	8.65	17.46
13	6.92	8.63	10.26	13.98
14	9.56	7.54	10.46	12.19
15	11.65	7.22	10.54	12.03
16	14.44	12.36	12.19	13.46
17	20.39	10.25	11.93	12.95
18	21.08	8.02	12.86	14.76
19	13.57	9.53	13.69	19.11
20	11.27	7.93	10.25	18.81
21	14.94	21.36	11.02	19.46
22	13.26	20.45	9.14	17.61
23	10.77	16.99	12.24	17.94
24	10.29	18.26	12.31	15.38
25	12.64	16.32	13.01	17.36
26	12.11	19.47	14.72	16.55

Table 7.1: Feature Selection mean error results for the CrossMatch dataset.

References

- [1] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.
- [2] S. Gayathri and V. Sridhar. FPGA implementation of orientation field estimation of fingerprint recognition process. *International Journal on Recent Trends in Engineering and Technology*, 11(1), 2014.
- [3] Samuel Fenker, Estefan Ortiz, and Kevin Bowyer. Template aging phenomenon in iris recognition. *Access, IEEE*, 1:266–274, 2013.
- [4] Kevin Bowyer. Accuracy of iris recognition systems degrades with increase in elapsed time. <https://spie.org/x90748.xml>, 2012.
- [5] Janeen Renaghan. Etched in stone. *Smithsonian Zoogoer*, August 1997.
- [6] Deepthi Bala. Biometrics and information security. In *Proceedings of the 5th annual conference on Information security curriculum development*, pages 64–66. ACM, 2008.
- [7] Anil Jain and Ajay Kumar. Biometrics of next generation: An overview. *Second Generation Biometrics*, 2010.
- [8] Adrian Pocovnicu. Biometric security for cell phones. *Informatica Economica*, 13(1):57–63, 2009.
- [9] Siddhesh Angle, Reema Bhagtani, and Hemali Chheda. Biometrics: A further echelon of security. In *UAE International Conference on Biological and Medical Physics*, 2005.
- [10] Yogendra Narain Singh and Sanjay Kumar Singh. Vitality detection from biometrics: state-of-the-art. In *2011 World Congress on Information and Communication Technologies (WICT)*, pages 106–111. IEEE, 2011.
- [11] Hugo Proença. Towards non-cooperative biometric iris recognition. *University of Beira Interior. Department of Computer Science*, 2006.
- [12] Mohmad Kashif Qureshi. Liveness detection of biometric traits. *International Journal of Information Technology and Knowledge Management*, 4:293–295, 2011.
- [13] João Monteiro. Robust iris recognition under unconstrained settings. Master’s thesis, Faculdade de Engenharia da Universidade do Porto, Portugal, 2012.
- [14] T Rakesh and MG Khogare. Survey of biometric recognition system for iris. *International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 6*, 2012.

- [15] Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez, Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia. Direct attacks using fake images in iris verification. In *Biometrics and Identity Management*, pages 181–190. Springer, 2008.
- [16] Nalini Ratha, Jonathan Connell, and Ruud Bolle. An analysis of minutiae matching strength. In *Audio-and Video-Based Biometric Person Authentication*, pages 223–228. Springer, 2001.
- [17] Bori Toth. Biometric liveness detection. *Information Security Bulletin*, 10(8):291–297, 2005.
- [18] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer, 2009.
- [19] Rod Seeley, Trent Stephens, and Philip Tate. *Essentials of anatomy & physiology*. St. Louis: Mosby-year book, 1996.
- [20] Kevin Bowyer, Karen Hollingsworth, and Patrick Flynn. Image understanding for iris biometrics: A survey. *Computer vision and image understanding*, 110(2):281–307, 2008.
- [21] Institute of Automation Chinese Academy of Sciences. Casia iris image database. <http://www.cbsr.ia.ac.cn/china/Iris%20Databases%20CH.asp>, 2004.
- [22] National Institute of Standards and Technology (NIST). Iris challenge evaluation. <http://www.nist.gov/itl/iad/ig/ice.cfm>, 2006.
- [23] S. Crihalmeanu, A. Ross, R. Govindarajan, L. Hornak, and S. Schuckers. A centralized web-enabled multimodal biometric database. In *Biometric Consortium Conference (BCC)*, Crystal City, Virginia, 2004.
- [24] Hugo Proença and Luís Alexandre. Ubiris: A noisy iris image database. In *Image Analysis and Processing–ICIAP 2005*, pages 970–977. Springer, 2005.
- [25] Hugo Proenca, Silvio Filipe, Ricardo Santos, Joao Oliveira, and Luis Alexandre. The ubiris. v2: A database of visible wavelength iris images captured on-the-move and at-a-distance. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 32(8):1529–1535, 2010.
- [26] Juliano Murari. Detecção de vivacidade em sistemas de reconhecimento de íris. Master’s thesis, Faculdade de Engenharia da Universidade do Porto, Portugal, 2013.
- [27] Multimedia University. MMU iris image database. <http://pesona.mmu.edu.my/~ccteo/>, 2004.
- [28] Ana Sequeira, João Monteiro, Ana Rebelo, and Helder Oliveira. Mobbio a multimodal database captured with an handheld device. volume 3, pages 133–139, 2014.
- [29] John Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 15(11):1148–1161, 1993.
- [30] Richard Wildes. Iris recognition: an emerging biometric technology. *Proceedings of the IEEE*, 85(9):1348–1363, 1997.
- [31] Using iris to enter the uk. <http://www.ukba.homeoffice.gov.uk/customs-travel/Enteringtheuk/usingiris/>.

- [32] John Daugman. Iris recognition border-crossing system in the UAE. *International Airport Review*, 8(2), 2004.
- [33] Ensuring uniqueness: Collecting iris biometrics for the unique ID mission. http://uidai.gov.in/UID_PDF/Working_Papers/UID_and_iris_paper_final.pdf.
- [34] Nexus pass application, US immigration visa & travel. <http://usa.immigrationvisaforms.com/travel/nexus-pass>.
- [35] Nexus - service Canada. http://www.servicecanada.gc.ca/eng/goc/nexus_highway.shtml.
- [36] About NEXUS. <http://cbsa-asfc.gc.ca/prog/nexus/about-sujet-eng.html>.
- [37] Iris recognition - Cairoamman bank. <http://www.cab.jo/service-details/61>.
- [38] Iris recognition finds favor. <http://www.bankersonline.com/articles/bhv10n02/bhv10n02a2.html>.
- [39] Don't blink: Iris recognition for biometric identification. <http://www.sans.org/reading-room/whitepapers/authentication/dont-blink-iris-recognition-biometric-identification-1341>, 2004.
- [40] Xiaofu He, Yue Lu, and Pengfei Shi. A new fake iris detection method. In *Advances in Biometrics*, pages 1132–1139. Springer, 2009.
- [41] Zhuoshi Wei, Xianchao Qiu, Zhenan Sun, and Tieniu Tan. Counterfeit iris detection based on texture analysis. In *19th International Conference on Pattern Recognition. ICPR 2008.*, pages 1–4. IEEE, 2008.
- [42] Ulf von Seelen. Countermeasures against iris spoofing with contact lenses. In *Biometric Consortium Conference BC*, 2005.
- [43] Javier Galbally, Jaime Ortiz-Lopez, Julian Fierrez, and Javier Ortega-Garcia. Iris liveness detection based on quality related features. In *5th IAPR International Conference on Biometrics (ICB)*, pages 271–276. IEEE, 2012.
- [44] Masashi Kanematsu, Hironobu Takano, and Kiyomi Nakamura. Highly reliable liveness detection method for iris recognition. In *SICE, 2007 Annual Conference*, pages 361–364. IEEE, 2007.
- [45] John Daugman. Anti-spoofing liveness detection. *University of Cambridge, computer laboratory, Cambridge.*, 2001.
- [46] John Daugman. Demodulation by complex-valued wavelets for stochastic pattern recognition. *International Journal of Wavelets, Multiresolution and Information Processing*, 1(01):1–17, 2003.
- [47] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang. Personal identification based on iris texture analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(12):1519–1533, 2003.

- [48] Xiaofu He, Shujuan An, and Pengfei Shi. Statistical texture analysis-based approach for fake iris detection using support vector machines. In *Advances in Biometrics*, pages 540–546. Springer, 2007.
- [49] Liveness competition 2013. <http://people.clarkson.edu/projects/biosal/iris/>.
- [50] Jay Doyle and Kevin Bowyer. Notre dame image dataset for contact lens detection in iris recognition, 2013.
- [51] Adam Czajka. Database of iris printouts and its application: Development of liveness detection method for iris recognition. In *Methods and Models in Automation and Robotics (MMAR), 2013 18th International Conference on*, pages 28–33. IEEE, 2013.
- [52] Juliano Murari, Ana Sequeira, and Jaime Cardoso. Iris liveness detection methods in mobile applications. In *Proceedings of International Conference on Computer Vision Theory and Applications (VISAPP)*, 2014.
- [53] Julian Fierrez, Javier Ortega-Garcia, Doroteo Torre Toledano, and Joaquin Gonzalez-Rodriguez. Biosec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 40(4):1389–1392, 2007.
- [54] Marie Sandström. Liveness detection in fingerprint recognition systems. 2004.
- [55] Yau Wei Yun. The ‘123’ of biometric technology. *Synthesis Journal*, 2002, 2002.
- [56] CI Watson and CL Wilson. NIST special database 4. *Fingerprint Database, National Institute of Standards and Technology*, 17, 1992.
- [57] CI Watson and CL Wilson. NIST special database 9, fingerprint database. *Special Database*, 1992.
- [58] CI Watson. NIST special database 10: Supplemental fingerprint card data (sfcd) for NIST special database 9. 1993.
- [59] Craig I Watson. Special database 14. In *S. Department of Commerce, NIST, Advanced Systems Division, Gaithersburg, Maryland*. Citeseer, 1993.
- [60] CI Watson. NIST special database 24 digital video of live-scan fingerprint data. 1998.
- [61] Michael Garriss and Michael McCabe. NIST special database 27: Fingerprint minutiae from latent and matching tenprint images. 2000.
- [62] Raffaele Cappelli, Matteo Ferrara, Annalisa Franco, and Davide Maltoni. Fingerprint verification competition 2006. *Biometric Technology Today*, 15(7):7–9, 2007.
- [63] BG Sherlock, DM Monro, and K Millard. Fingerprint enhancement by directional fourier filtering. In *Vision, Image and Signal Processing, IEE Proceedings-*, volume 141, pages 87–94. IET, 1994.
- [64] Ahmed Abutaleb and M Kamel. A genetic algorithm for the estimation of ridges in fingerprints. *Image Processing, IEEE Transactions on*, 8(8):1134–1139, 1999.

- [65] Yuheng Zhang and Qinghan Xiao. An optimized approach for fingerprint binarization. In *Neural Networks, 2006. IJCNN'06. International Joint Conference on*, pages 391–395. IEEE, 2006.
- [66] Takahiro Hatano, Takuya Adachi, Satoshi Shigematsu, Hiroki Morimura, Shigehiko Onishi, Yukio Okazaki, and Hakaru Kyuragi. A fingerprint verification algorithm using the differential matching rate. In *Pattern Recognition, International Conference on*, volume 3, pages 30799–30799. IEEE Computer Society, 2002.
- [67] Tsai-Yang Jea and Venu Govindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38(10):1672–1684, 2005.
- [68] Yangyang Zhang, Xin Yang, Qi Su, and Jie Tian. Fingerprint recognition based on combined features. In *Advances in Biometrics*, pages 281–289. Springer, 2007.
- [69] Ton Van der Putte and Jeroen Keuning. Biometrical fingerprint recognition: don't get your fingers burned. In *Smart Card Research and Advanced Applications*, pages 289–303. Springer, 2000.
- [70] Luca Ghiani, Abdenour Hadid, Gian Luca Marcialis, and Fabio Roli. Fingerprint liveness detection using binarized statistical image features. In *IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, pages 1–6. IEEE, 2013.
- [71] David Yambay, Luca Ghiani, Paolo Denti, Gian Luca Marcialis, Fabio Roli, and S Schuckers. LivDet 2011—fingerprint liveness detection competition 2011. In *5th IAPR International Conference on Biometrics (ICB)*, pages 208–215. IEEE, 2012.
- [72] Luca Ghiani, Gian Luca Marcialis, and Fabio Roli. Fingerprint liveness detection by local phase quantization. In *21st International Conference on Pattern Recognition (ICPR)*, pages 537–540. IEEE, 2012.
- [73] Timo Ojala, Matti Pietikainen, and Topi Maenpaa. Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 24(7):971–987, 2002.
- [74] Diego Gragnaniello, Giovanni Poggi, Carlo Sansone, and Luisa Verdoliva. Fingerprint liveness detection based on weber local image descriptor. In *Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2013 IEEE Workshop on*, pages 46–50. IEEE, 2013.
- [75] Gian Luca Marcialis, Aaron Lewicke, Bozhao Tan, Pietro Coli, Dominic Grimberg, Alberto Congiu, Alessandra Tidu, Fabio Roli, and Stephanie Schuckers. First international fingerprint liveness detection competition—livdet 2009. In *Image Analysis and Processing—ICIAP 2009*, pages 12–23. Springer, 2009.
- [76] BG Warwante and Mr SA Maske. Wavelet based fingerprint liveness detection. *International Journal of Engineering Research and Applications*, 2(2):1643–1645, 2012.
- [77] Bozhao Tan and Stephanie Schuckers. Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise. *Pattern Recognition*, 43(8):2845–2857, 2010.
- [78] Bozhao Tan and Stephanie Schuckers. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06.*, pages 26–26. IEEE, 2006.

- [79] Javier Galbally, Fernando Alonso-Fernandez, Julian Fierrez, and Javier Ortega-Garcia. A high performance fingerprint liveness detection method based on quality related features. *Future Generation Computer Systems*, 28(1):311–321, 2012.
- [80] Javier Galbally, Julian Fierrez, Fernando Alonso-Fernandez, and Marcos Martinez-Diaz. Evaluation of direct attacks to fingerprint verification systems. *Telecommunication Systems*, 47(3-4):243–254, 2011.
- [81] Luca Ghiani, David Yambay, Valerio Mura, Simona Tocco, Gian Luca Marcialis, Fabio Roli, and Stephanie Schuckers. Livdet 2013 fingerprint liveness detection competition 2013. In *2013 International Conference on Biometrics (ICB)*, pages 1–6. IEEE, 2013.
- [82] David G Lowe. Object recognition from local scale-invariant features. In *Seventh IEEE international conference on Computer vision*, volume 2, pages 1150–1157. Ieee, 1999.
- [83] Hui Zhang, Zhenan Sun, and Tieniu Tan. Contact lens detection based on weighted LBP. In *20th International Conference on Pattern Recognition (ICPR)*, pages 4279–4282. IEEE, 2010.
- [84] Konstantinos G. Derpanis. Computer vision related note - York University. <http://dweller.cvr.yorku.ca/members/gradstudents/kosta/compvis/index.html>.
- [85] Joana Fonseca. Pre-cads in breast cancer. Master’s thesis, Faculdade de Engenharia da Universidade do Porto, Portugal, 2013.
- [86] Robert M Haralick, Karthikeyan Shanmugam, and Its’hak Dinstein. Textural features for image classification. *IEEE Transactions on Systems, Man and Cybernetics*, (6):610–621, 1973.
- [87] Luca Ghiani, Gian Luca Marcialis, and Fabio Roli. Experimental results on the feature-level fusion of multiple fingerprint liveness detection algorithms. In *Proceedings of the on Multimedia and security*, pages 157–164. ACM, 2012.
- [88] Richard L. White. Methods for classification. <http://sundog.stsci.edu/rick/SCMA/node1.html>.
- [89] Chih-Chung Chang and Chih-Jen Lin. Libsvm: a library for support vector machines. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2(3):27, 2011.
- [90] Chris Ding and Hanchuan Peng. Minimum redundancy feature selection from microarray gene expression data. *Journal of bioinformatics and computational biology*, 3(02):185–205, 2005.
- [91] Gavin Brown. A new perspective for information theoretic feature selection. In *International Conference on Artificial Intelligence and Statistics*, pages 49–56, 2009.
- [92] Jeff Schneider. Cross validation. <http://www.cs.cmu.edu/~schneide/tut5/node42.html>, 1997.
- [93] Luigi Rosa. LBP face recognition system matlab code. <http://www.advancedsourcecode.com/lbpfacedem.zip>.

- [94] Notre Dame University Clarkson University and Warsaw University of Technology. Liveness Detection-iris competition 2013. IEEE BTAS 2013, 2013. <http://people.clarkson.edu/projects/biosal/iris/results.php>.