Universidad Autónoma de Madrid

Escuela politécnica superior

Proyecto fin de carrera

RECONOCIMIENTO BIOMÉTRICO DE IRIS BASADO EN CARACTERÍSTICAS SIFT

Ingeniería de Telecomunicación

Virginia Ruiz Albacete

Septiembre 2010

RECONOCIMIENTO BIOMÉTRICO DE IRIS BASADO EN CARACTERÍSTICAS SIFT

AUTOR: Virginia Ruiz Albacete
TUTOR: Fernando Alonso Fernández
PONENTE: Javier Ortega García

Área de Tratamiento de Voz y Señales
Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Septiembre 2010

Abstract

Abstract

This M.Sc. Thesis presents the study, implementation and evaluation of an iris-based automatic recognition system based of SIFT features. We also carry out an study of vulnerabilities of the developed SIFT matcher to direct attacks using fake iris images. We use for our experiments the BioSec Baseline database and a fake iris database developed from the first one, both freely available upon request. The study of vulnerabilities done in the framework of this Project has also included the acquisition of the mentioned fake iris database.

We first start by describing the existing methods for iris recognition. After an introduction to biometrics and a review of the state of the art of iris-based systems, an implementation of the selected algorithm is performed, including the proposal of some improvements for the system.

In the experimental section, we first evaluate separately the performance of the different stages of the implemented system in order to optimize them. Studies have mainly focused on the two principal steps, which are feature extraction and score matching. The obtained results have been compared with a freely available traditional iris recognition system, which is used as baseline system. The main novelty of the proposed system with respect to traditional approaches is that it does not need to transform the ring-shaped region of the iris to polar coordinates. This avoids the need of a very accurate segmentation, which can be difficult with non-ideal images.

Once the system has been optimized, its robustness to direct attacks has been tested through a developed fake iris database. The results are once more compared to those obtained with the baseline iris recognition system. Lastly, our conclusions and some future directions to improve the implemented system are presented.

Key words

Biometrics, image processing, pattern recognition, iris recognition, Shift Invariant Feature Transform, direct attacks to biometric systems, fake iris.

Resumen

Este Proyecto presenta el estudio, implementación y evaluación de un sistema automático de reconocimiento de iris basado en características SIFT. También se lleva a cabo un estudio de vulnerabilidades antes ataques directos del sistema, a través de imágenes falsas de iris. Como bases de datos para la experimentación se emplea BioSec-Baseline y una base de datos falsa desarrollada a partir de la misma, ambas de libre acceso a la comunidad científica. El estudio de vulnerabilidades en el marco de trabajo de este Proyecto también incluye la adquisición de la bases de datos de iris sintéticos previamente mencionada.

Como punto de partida, se toman una serie de características y sistemas de reconocimiento propuestos en la literatura. Tras una introducción a la biometría y un estudio del estado del arte en reconocimiento de iris, se hace una implementación del método elegido, incluyendo la propuesta de mejoras en el sistema.

En la sección experimental se han llevado a cabo pruebas de cada una de las etapas del sistema, de modo que podamos evaluar el sistema desarrollado de forma detallada, con sus puntos fuertes y débiles. Los experimentos se han centrado en la mejora independiente de las dos etapas más importantes, extracción de características y matching scores. Dichos resultados han sido comparados con un sistema de reconocimiento biométrico de iris tradicional y de libre disposición, el cual es usado como sistema de referencia. La mayor novedad del sistema propuesto es que éste no necesita transformar la región circular del iris a coordenadas polares, eliminando la necesidad de una precisa segmentación, que puede ser difícil en imágenes no ideales.

Además de la evaluación del rendimiento global del sistema desarrollado y una vez hallados los parámetros de funcionamiento óptimos, se presenta un estudio de su resistencia frente ataques directos a través de una base de datos de iris falsos desarrollada. Los resultados son comparados una vez más con el método de reconocimiento de iris de referencia. Finalmente, se presentan las conclusiones y se proponen líneas de trabajo futuras.

Palabras Clave

Biometría, procesamiento de imágenes, reconocimiento de patrones, reconocimiento de iris, SIFT, ataques directos a sistemas biométricos, iris falsos.

Agradecimientos

Aprender a volar es una tarea complicada; pero todo aprendizaje tiene su fin y llega el momento de mirar atrás y agradecer, con cariño y respeto, a todos aquellos que nos enseñaron a alzar el vuelo. En primer lugar agradecer a mi ponente Javier Ortega, por acogerme en la familia *ATVSiana* y darme la oportunidad de realizar mi PFC rodeada de las mejores influencias. Gracias a cada uno de vosotros, esas cuatro paredes se convirtieron en lugar de apoyo y referencia durante dos años fantásticos. En especial, a mi *Maestro* (y gran piloto de la F1), Fernando Alonso, que me ha indicado siempre la dirección en la que sopla el viento; no existen palabras suficientes para agradecer todo tu esfuerzo. Con cariño especial, agradecer a Peter su paciencia, disponibilidad y ayuda incondicional, tanto en temas profesionales como personales. Dani, Gal, Manu, Julián, Javi, Iñaki y como no, Almu y Ali, ¡*babies* for ever! Compañeros y fuente de inspiración nunca me olvidaré de vosotros.

Es el trabajo de muchos años el que hace posible la escritura de estos agradecimientos. Desde los profesores que asentaron las bases científicas en mi (Pilar, Feli y Carlos, ¡vaya pilota sería hoy sin vosotros!), hasta los que que me enseñaron las *técnicas de vuelo avanzadas*, a través de un contacto cercano y profesional. En especial agradecer a Jesús y a Susana sus sabios consejos. Sólo los años reflejarán los frutos de todos vuestros esfuerzos.

Planear sobre lo desconocido permite apreciar mejor lo que nos rodea. A esa gente que en 5 años han pasado de ser perfectos desconocidos a amigos. Vuestra compañía ha reemplazado los malos momentos de estos años por las fantásticas experiencias que hemos vivido juntos. Desde los cercanos (Davor, ¡que ganas de perderte de vista!), hasta los que se han convertido en familia (primo, ¡vivan tus croquetas!), incluyendo aquellos que ya no caminan a nuestro lado (nunca te olvidaré Luis), gracias por formar parte de mi vida. No me quiero olvidar de esa panda de *informáticos* que tanta ayuda me han prestado... ¡sois los culpables de que se me oiga reír desde reprografía!

También quiero agradecer a ese grupo extraordinario de personas *de siempre* que con tanto cariño me prestan su apoyo incondicional y hacen que cada momento juntos merezca la pena. En especial a mis niñas Mery, Maka, Bea, Marta, Peggy; ¡tantos años juntas hacen que no me pueda imaginar la vida sin vosotras! A mi gran amigo Albert, con el que nunca me cansaré de compartir buenas cenas. Y por supuesto, a esa personita tan especial que siempre encuentra un rayito de luz en la oscuridad. ¡Orgullosa y agradecida de tenerte a mi ladito Diegui! No sabría seguir sin ti... *I do it for you.*

No me olvido de los grandes pilares de mi vida. A mi familia, que con tanta confianza me ha apoyado siempre, ¡ya hay un Ingeniero en la familia! A mis abuelas y tías, gracias por las velitas, la preocupación y los mimos. Y como no, a las piezas fundamentales de mi rompecabezas, gracias por aguantarme en mis momentos de euforia y de bajón, por ayudarme siempre a buscar una solución, por apoyar todas mis decisiones, por no dejarme rendirme, y por ayudarme a levantarme tras cada caída. Pocas hijas están tan orgullosas de sus padres. Finalmente, agradecer a mi *sunshine*; has dejado de ser mi hermana para convertirte en mi amiga, consejera y confidente. Que por muchos kilómetros que nos separen nunca perdamos esa conexión especial *BigSis*.

MUCHAS GRACIAS

Nada en el mundo sustituye a la constancia. El talento no la sustituye, pues nada es más corriente que los inteligentes frustrados. El genio tampoco, ya que resulta tópico el caso de los genios ignorados. Ni siquiera la educación sustituye a la constancia, pues el mundo está lleno de fracasados bien educados. Solamente la constancia y la decisión lo consiguen todo.

Baltasar Gracián

A mi madre

El trabajo de investigación que ha dado lugar a este Proyecto Fin de Carrera fue desarrollado en el *Área de Tratamiento de Voz y Señales*, Departamento de Ingeniería Informática, Escuela Politécnica Superior, Universidad Autónoma de Madrid.

Índice general

List of Figures

List of Tables

1 Introduction

1.1. Motivation of the Project

The increasing interest on biometrics is related to the swift development of the information society and the number of important applications where a correct assessment of identity is a crucial point. The term *biometrics* refers to automatic recognition of an individual based on what he/she *is*, rather than on something that you *know* (password, PIN) or something that you *have* (card, key, etc.). In biometric systems, users do not need to remember passwords or PINs (which can be forgotten) or to carry cards or keys (which can be stolen), which provides a fast and reliable recognition technique.

Biometric systems can be classified as those that use morphological or anatomical traits, and those that use behavioral or conductual traits for his/her identification [3]. Fingerprints, hand geometry, iris or DNA are some examples that fall under the classification of anatomical traits. They are characterized by a lesser variability over time, although their capture is more invasive since they require the user's cooperation. On the other hand, behavioral traits such as signature, writing or voice are less intrusive although they require an specific realization to be acquired since they are not present all the time (e.g. to sign or to speak), and their precision is lower due to their variability (based on natural evolution across time or even user's mood at some specific moment).

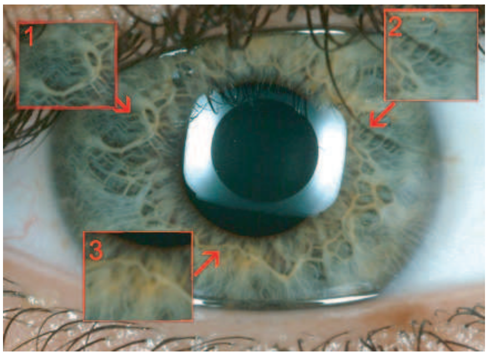


Figure 1.1: Characteristics that allow iris recognition.

Among all biometric techniques, iris recognition has been traditionally regarded as one of the most reliable and accurate biometric identification system available [3, 4]. The human iris is a colored ring between the pupil and the sclera, which is made up of a number of rods, crowns, folds, etc. known as the "iris texture". These visible features are unique and distinctive for every individual, which allows a reliable recognition (Figure 1.1). Furthermore, being an externally visible, yet protected organ whose unique pattern remains stable throughout adult life, iris recognition becomes a very attractive technique for biometric identification.

In spite of these advantages, biometric systems have some drawbacks [5]: *i*) the lack of secrecy (e.g. everybody knows our face or could get our fingerprints), and *ii*) the fact that a biometric trait can not be replaced (if we forget a password we can easily generate a new one, but no new fingerprint can be generated if an impostor "steals" it). Moreover, biometric systems are vulnerable to external attacks which could decrease their level of security. In [6] Ratha *et al.* identified and classified eight possible attack points to biometric recognition systems.

Traditional iris recognition approaches approximates iris boundaries as circles. The ring-shaped region of the iris is then transferred to a rectangular image in polar coordinates, with the pupil center being the center of the polar coordinates [7]. This transfer normalizes the distance between the iris boundaries due to contraction/dilation of the pupil, the camera zoom or the camera to eye distance. When converting an iris region to polar coordinates, it is necessary a very accurate segmentation in order to create a similar iris pattern mapping between images of the same eye [8]. Features are then extracted from the rectangular normalized iris pattern. For this purpose, a number of approaches have been proposed in the literature [9], e.g.: Gabor filters, log-Gabor filters, Gaussian filters, Laplacian-of-Gaussian filters, wavelet transforms, etc.

With these ideas in mind, we present in this Project an iris recognition system based on the Scale Invariant Feature Transformation (SIFT). The main differences between traditional iris recognition approaches and the SIFT technique are: i) there is no need to transform the iris region to polar coordinates, avoiding the inherent problems of this procedure with non-ideal images; and ii) the features used for recognition are extracted from local distinctive regions only (i.e. points), rather than encoding the whole iris region by filtering. The SIFT system is compared with a traditional iris recognition approach, including their fusion in order to show their complementary behavior. We also carry out an study of direct attacks to the two evaluated systems using fake iris images, pointing out their vulnerability and thus, the need of appropriate countermeasures.

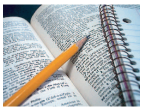
1.2. Objectives and methodology

One of the drawbacks of traditional iris recognition approaches is that the transformation to polar coordinates can fail with non-cooperative or low quality data (e.g. changes in the eye gaze, non-uniform illumination, eyelashes/eyelids occlusion, etc.) [8]. In this Project, we implement the Scale Invariant Feature Transformation (SIFT) [2] for its use in biometric recognition using iris images. SIFT extracts repeatable characteristic feature points from an image and generates descriptors describing the texture around the feature points. The SIFT technique has already demonstrated its efficacy in other generic object recognition problems, and it has been recently proposed for its use in biometric recognition systems based on face [10, 11], fingerprint [12] and iris images [8].

The objective of this Project is to study, develop and implement a system based on SIFT features, to allow an automatic iris identification. The starting point of our work will be based on the description of the SIFT algorithm presented in [2]. This system will be then modified to fulfill our requirements, and once implemented, it will be optimized and its behavior will be tested. During these evaluations we have used the BioSec database [13], available in the ATVS group, which has been widely used in previous reference publications. The system used as reference to measure the performance of the developed system is also freely available and used in some other previous works found in the literature.

Besides, this Project aims to deal with the security issues of the iris recognition systems due to direct attacks. For this purpose we have built a database with synthetic iris images generated from users of the BioSec multi-modal baseline corpus [13], and once more, the implemented system will be tested an its performance compared to traditional reference iris recognition systems.

To do so, the work methodology has been divided in 4 parts as follows:



Formation: in order to obtain the expected results, a basic knowledge of principles of biometrics is essential. The reading of international scientific publications has enabled a synthesis of the state of the art in biometric recognition systems. Iris recognition systems and their vulnerability have covered most of the last stage of formation.

Investigation: after a first contact with biometrics, it is necessary to deeply study the algorithms and developments behind the different methodologies found in the literature. This allows a subsequent enrichment and improvement of our implemented system.

Implementation: the final objective of this Project is to obtain a practical implementation of the iris system and its evaluation. Based on the previous study, we can recreate and optimize the reference system, to reach our goal.

Writing and publications: even though an continuous documentation has been gathered throughout the work, the main writing part of the Project has been done after the testing and evaluations were concluded. Meanwhile, our studies have been published in international scientific conferences [14, 15].

1.3. Memory organization

The present work describes the development of an automatic biometric iris-based recognition system, its evaluation and robustness to attacks. It is structured as follows

The chapter 1 contains the introduction, motivation, objectives, methodology and summary of the contributions of this M.Sc. Thesis.

Chapter 3 contains an overview of the principles of biometrics. To do so, its main characteristics, the different classifications of the biometric traits and the different types of biometric systems are introduced. The general structure of these systems is also included, along with their advantages, applications, operational modes and limitations, that altogether allow their evaluation. Finally, some issues related to privacy and society acceptance are presented.

After an introduction to the biometrics world, we have realized a detailed state of the art of iris recognition, shown in the chapter 4. After a historical review of the most relevant facts, since its appearance to nowadays, an objective study of the human eye's anatomy is exposed, followed by other related iris-related sciences, such as iridology. All these facts are relevant to develop a proper understanding of the most important methods of acquisition, segmentation, normalization and extraction explained next. Different matching and comparing algorithms are also studied. The chapter ends with a brief overview of the main drawbacks and challenges of iris, as well as a summary of the iris technological contests and the existing databases.

The chapter 5 details the developed system based of Shift Invariant Feature Transform points, describing in an organized way the implemented algorithms for each block of the system. The codes that compose the system have been programmed in a PC using Matlab® .

Results and further discussion are reported in Chapter 6, which includes a description of the framework, the used database and the experimental protocol. In more detail, this chapter includes the proceedings for the system optimization and the comparisons to the reference system. Besides, we have included the description of the developed fake iris database, that will allow to check the robustness of our system to direct attacks.

Conclusions are finally drawn in Chapter 8 along with the possible future work that derives from this study.

The references of this Project can be found at the end of it, in the Bibliography Section. This work is completed by a number of appendix with the Project budget, the schedule of conditions and the published articles.

1.4. Contributions

The contributions of this M.Sc. Thesis for the biometric recognition group (ATVS) and the scientific community can be summarized in the following points:

- Summary of the state of the art of the different methodologies used in iris-based biometric recognition systems.
- Study of the challenges and vulnerabilities to direct attacks of iris-based verification systems.
- Development and implementation of an iris recognition system, based of Shift Invariant Feature Transform features, following previos works of the literature.
- Adjustment, training, optimization and improvement of the developed system to use it as a reliable iris recognition biometric technique.
- Evaluation of the results obtained through our system including, comparison and combination with the reference system, to draw the appropriate conclusions about its viability and performance.
- Development of a database of synthetic iris images from real iris of the BioSec baseline database.
- Analysis of the effects of direct attacks in the developed SIFT system and comparison of the results to the effect of these attacks on traditional iris-based recognition systems.

We want to point out the publication of the studies concerning the direct attacks and the implemented system based on SIFT feature in scientific revisited conferences [14, 15].

2

Introducción

2.1. Motivación del proyecto

El crecimiento de la sociedad de la información experimentado en los últimos años, y el consiguiente incremento de los requerimientos de seguridad, han dado lugar a un rápido desarrollo de sistemas automáticos de identificación personal basados en técnicas biométricas. En la actualidad, el uso de este tipo de de técnicas está cobrando gran relevancia, ya que la biometría supone una forma sencilla y segura de identificación de personas. Una de sus principales ventajas consiste en que los rasgos biométricos en general son más difíciles de duplicar o falsificar ya que, a diferencia de los métodos comúnmente utilizados, no se basan en lo que cada individuo *posee* (por ejemplo el DNI o una llave), que puede ser perdido, o *recuerda* (por ejemplo un PIN), que puede ser olvidado, para confirmar o establecer su identidad, sino en algo que el individuo *es*.

Las técnicas biométricas se pueden clasificar en aquellas que usan rasgos biométricos morfológicos o anatómicos, y las que usan características de comportamiento o conducta para su identificación [3]. Entre los rasgos biométricos anatómicos se encuentran, por ejemplo, la huella dactilar, la geometría de la mano, el iris y el ADN entre otros. Se caracterizan por una menor variabilidad a lo largo del tiempo, pero su adquisición es más invasiva y requiere la cooperación de los sujetos. Por el contrario, los rasgos biométricos de comportamiento o conducta, como pueden ser la voz, la firma o la escritura, requieren una realización (como el firmar o el hablar) ya que no están presentes de modo permanente. Sin embargo, son menos invasivos, aunque la exactitud de la identificación es menor debido a la variabilidad de los patrones de comportamiento (por la evolución temporal natural o incluso al estado de ánimo del usuario en un momento concreto).

Entre todos los rasgos biométricos, el reconocimiento del iris es considerado como uno de los medios más precisos y fiables [3, 4]. El iris humano consiste en un anillo situado entre la pupila y la esclera, el cual contiene gran cantidad de características muy precisas como bastoncillos, coronas, pliegues, etc. Estas características visibles, que son conocidas como textura del iris, son únicas y propias de cada individuo. Además, gracias a la protección que proporciona la pupila, el iris de una persona es muy estable a lo largo de toda su vida y, al mismo tiempo, se trata de un órgano visible externamente, por lo que permite una identificación no invasiva (Figura 2.1). Todo ello ha suscitado un gran interés por el reconocimiento basado en iris en los últimos años, debido a sus posibilidades en el campo de seguridad y a su uso, por ejemplo, en aeropuertos y cajeros.

A pesar de estas ventajas, los sistemas biométricos también suponen una serie de riesgos [5]: *i*) falta de privacidad (p.e. todo el mundo conoce nuestra cara o podría adquirir nuestra huella), y *ii*)

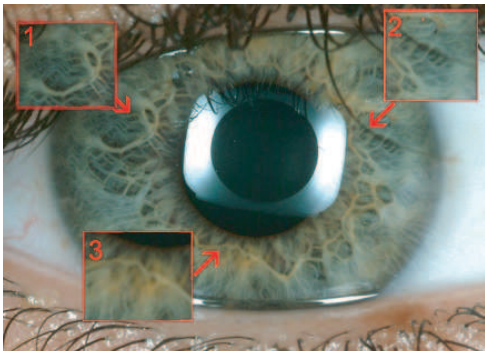


Figure 2.1: Características del iris que permiten su reconocimiento.

el hecho de que un rasgo biométrico no pueda ser sustituido (si nos olvidamos de una contraseña, esta puede ser regenerada, pero no se puede sustituir una huella que ha sido "robada" por un impostor). Además, los sistemas biométricos son vulnerables a ataques externos que podrían decrementar su nivel de seguridad. En [6] Ratha *et al.* identificó y clasificó ocho posibles puntos de ataque en sistemas de reconocimiento biométrico.

Los sistemas tradicionales de reconocimiento de iris se basan en una aproximación circular de sus límites, que es posteriormente transformada en una imagen rectangular a través de las coordenadas polares. Esta transformación, en la que el centro de la pupila indica el centro de las coordenadas [7], normaliza la distancia entre los límites del iris debido a la contracción y dilatación de la pupila, el zoom de la cámara o la distancia de la cámara al ojo. Sin embargo, al convertir una región del iris a coordinadas polares, es necesario que la segmentación sea muy precisa para lograr que la comparación entre modelos de un mismo ojo sea muy parecida [8]. El siguiente paso se centra en la extracción de características del modelo rectangular normalizado del iris. Para ello se han propuesto numerosas aproximaciones en la literatura [9], p.e.: filtros de Gabor, filtros de log-Gabor, filtros Gaussianos, filtros Laplacianos de Gaussianos, transformadas de wavelets y otros.

Con todo ello en mente, en este Proyecto presentamos un sistema de reconocimiento de iris basado en características SIFT. Las principales diferencias de este sistema con respecto a los anteriores son: *i*) no requiere la transformación a coordenadas polares de la región del iris, evitando los problemas inherentes de esta técnica en imágenes no ideales; y *ii*) las características usadas para el reconocimiento son extraídas únicamente de regiones locales distintivas, es decir puntos, en vez de codificar a través del filtrado toda la región del iris. El sistema SIFT es comparado con una técnica de reconocimiento de iris tradicional, incluyendo su fusión para demostrar su complementariedad. Además, a través de imágenes falsas, llevamos a cabo un estudio de ataques directos a los dos sistemas evaluados, resaltando sus vulnerabilidades y, por tanto, la necesidad de medidas apropiadas.

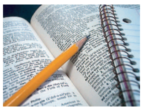
2.2. Objetivos y metodología

Una de las principales desventajas de los sistemas tradicionales de reconocimiento de iris es que la transformación a coordenadas polares puede fracasar cuando se trabaja con usuarios no cooperativos o información de baja calidad (debida por ejemplo a cambios en la orientación de la mirada, iluminación no uniforme u oclusión producida por pestañas ó párpados durante la adquisición) [8]. El presente Proyecto se centra en el estudio e implementación de un sistema de reconocimiento de iris basado en características conocidas como SIFT [2]. A través de este método es posible extraer puntos característicos y discriminantes, y generar descriptores que caractericen de forma única e inequívoca su textura circundante. Esta metodología ha demostrado su eficacia en otros campos de reconocimiento genérico de objetos, aunque solo recientemente ha sido considerada con fines biométricos de cara [10, 11], huella dactilar [12] e imágenes de iris [8].

Este proyecto tiene como objetivo estudiar, desarrollar, implementar y documentar un sistema basado en características SIFT que permita la identificación automática del iris en base al estado del arte actual. Como punto de partida se tomará la descripción del algoritmo presentado en [2], el cual está caracterizado por una serie de parámetros. Dicho sistema ha sido modificado para acomodarse a los nuevos requisitos, por lo que una vez implementado, será optimizado a través de diversos experimentos y, a continuación, será evaluado respecto al sistema original. Para estas evaluaciones, se ha hecho uso de la base de datos BioSec [13], disponible en el grupo ATVS, ampliamente utilizada en publicaciones previas de referencia. Igualmente, se ha utilizado un sistema de libre acceso, usado en otros trabajos previos, disponibles en la literatura, que servirá como referencia para medir el rendimiento del sistema desarrollado.

Además, en este Proyecto se pretende abarcar los asuntos de seguridad de los sistemas de reconocimiento de iris debido a ataques directos. Para ello, se desarrollará una base de datos de iris sintéticos generados a partir de usuarios de la base de datos BioSec [13], y se pondrá a prueba el sistema desarrollado, comparándolo una vez más con los resultados de sistemas de referencia.

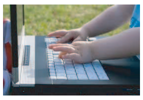
Para ello hemos dividido la metodología de trabajo en 4 bloques:



Formación: un primer contacto a la biometría es fundamental para obtener los conocimientos básicos sobre el estado del arte actual. Gracias a la lectura de publicaciones científicas internacionales de referencia ha sido posible presentar una síntesis del estado del arte en sistemas de identificación biométrica. La etapa final de formación fue especializada en reconocimiento de patrones de iris y ataques a dichos sistemas.

Investigación: tras una primera aproximación, es necesario estudiar en detalle los algoritmos y razonamientos matemáticos que se encuentran detrás de las distintas metodologías. Esto permitirá aportar nuevas ideas y soluciones a la implementación final.

Desarrollo: el objetivo final es obtener una implementación práctica de un sistema de iris y su posterior evaluación. Apoyándonos en la literatura existente y las investigaciones llevadas a cabo, nos es posible recrear y optimizar el sistema deseado para nuestros objetivos.



Escritura y publicaciones: a pesar de realizar una escritura progresiva del trabajo realizado en este Proyecto, la mayor parte de esta etapa se ha realizado al concluir el periodo de desarrollo y pruebas. Resultados e investigaciones intermedias han sido divulgadas a través de publicaciones internacionales y conferencias científicas especializadas [14, 15].

2.3. Organización de la memoria

El presente trabajo describe el desarrollo de un sistema automático de reconocimiento biométrico basado en iris, su evaluación y estudio de robustez frente ataques. Su organización es la siguiente:

El Capítulo 2 contiene la introducción, la motivación, los objetivos, la metodología y un resumen de las aportaciones de este Proyecto Fin de Carrera.

En el Capítulo 3 se realiza una revisión de las bases de la biometría. Para ello se introducen sus principales características, las distintas clasificaciones de los rasgos biométricos en función de sus particularidades y los distintos sistemas biométricos. De estos últimos se incluye un análisis de la estructura general que debe seguir todo sistema biométrico junto con sus ventajas, aplicaciones, modos de operación y limitaciones, incluyendo las diferentes formas de medir un sistema de este tipo. Finalmente, se comentan algunas cuestiones relativas a la privacidad y aceptación en la sociedad.

Tras esta introducción al mundo de la biometría, realizamos una revisión detallada del estado del arte en reconocimiento de iris en el Capítulo 4, tema principal de este trabajo. Un recorrido histórico por los hechos más relevantes que han motivado y acompañado al desarrollo de esta tecnología, desde su nacimiento hasta la fecha actual, precede a un estudio objetivo de la anatomía del ojo humano y la consideración de otras ciencias relacionadas que estudian el iris, como la iridología. Todos estos factores son relevantes para entender los métodos de adquisición, segmentación, normalización y extracción más importantes expuestos a continuación. También se estudian los distintos algoritmos de codificación de la información de iris, alineamiento de patrones y métodos de comparación de los mismos. Para finalizar, el Capítulo hace un breve repaso de la problemática del iris así como de sus retos. También se resumen las competiciones tecnológicas de iris, así como las bases de datos existentes.

El Capítulo 5, se detalla el sistema basado en características SIFT desarrollado en este proyecto, describiendo de forma ordenada los algoritmos implementados en cada una de las etapas del sistema. Los algoritmos que conforman el sistema están programados en un PC utilizando Matlab® .

La evaluación del sistema desarrollado se expone en el Capítulo 6, que incluye una descripción del marco de trabajo, la base de datos usada y el protocolo seguido para la obtención de resultados. De forma más detallada, en él se encuentran los procedimientos seguidos para su optimización, y las comparaciones realizadas con el sistema de referencia. En este apartado también se encuentra la descripción de la base de datos de iris falsos, creada para comprobar la robustez del sistema ante ataques directos. Gracias a ella podemos determinar su eficacia y compararla con aquella de los sistemas de reconocimiento de iris tradicionales, midiendo el rendimiento global del sistema desarrollado.

La presentación de resultados y conclusiones se presenta en el Capítulo 8, donde se plantean además posibles vías para trabajo futuro.

Las referencias consultadas para la consecución de este Proyecto pueden encontrarse al final del tomo, en la Sección de Bibliografía. Este trabajo se completa con una serie de anexos en los que figuran el presupuesto, el pliego de condiciones, y las publicaciones derivadas de este trabajo.

2.4. Contribuciones

Las contribuciones de este Proyecto para el grupo de reconocimiento biométrico ATVS y la comunidad científica puede resumirse en los siguientes aspectos:

- Resumen del estado del arte de las distintas metodologías usadas en sistemas de reconocimiento biométrico basados en iris.
- Estudio de las vulnerabilidades y retos de los sistemas biométricos.
- Implementación y desarrollo de un sistema de reconocimiento de iris basado en las características SIFT siguiendo trabajos previos encontrados en la literatura.
- Adaptación, entrenamiento, optimización y mejora del sistema desarrollado para enfocarlo al reconocimiento biométrico de iris.
- Evaluación de los resultados obtenidos con nuestro sistema, incluyendo una comparación y una combinación con el sistema de referencia.
- Creación de una base de datos de imágenes de iris sintéticas a partir de los iris reales de la base de datos BioSec.
- Análisis del comportamiento del sistema de reconocimiento de iris desarrollado ante ataques directos con imágenes de iris falsas, en contraposición a los resultados obtenidos con sistemas de reconocimiento de iris tradicionales.

Señalar que los estudios de vulnerabilidades de sistemas biométricos ante ataques directos y el sistema basado en características SIFT implementado, han sido aceptados como artículos de congreso con revisión científica [14, 15].

3 Introduction to Biometrics

In today's networked and rapidly changing society, the need for reliable, simple, flexible and secure systems is a great concern and a challenging issue. Day by day security breaches and transaction frauds increase, so the need for secure identification and personal verification technologies is becoming a great concern. It is necessary that all interactions and transactions with digital systems and devices are both convenient and secure. However, there is generally an inverse relationship between security and convenience. Awareness of security issues is rapidly increasing among society leading to new technologies and innovations. Personal identification can be divided in three general groups: based on something that the individual *knows* (e.g., password or PIN), on something that he/she *has* (e.g., key, card) or something that he/she *is* (e.g., the face). ***Biometric recognition***, which is described as the science of recognizing an individual based on his/her anatomical or behavioral traits, belongs to this last group [3, 4]. It presents several advantages over traditional security methods, since it does not require to memorize a PIN, which can be forgotten, or to carry cards, which can be stolen or lost.

3.1. Characteristics of Biometrics

The word biometric comes from the Greek terms *bios* (life) and *metrikos* (measure). Humans have intuitively used body characteristics, such as face or voice, for thousands of years to recognize each other. The use of these human traits for identification started back in the ancient Egypt. The first fingerprint identification records come from ancient China and nowadays, these rudimentary means of identification have evolved to systems in effect around the world such as in the United States and Europe. In the mid-19th century, the first body measurements oriented to criminal identification were used by Alphonse Bertillon [16]. Although biometrics emerged from its extensive use in law enforcement to identify criminals, it is being increasingly used today for individual recognition in a large number of civilian applications. There are two main classes into which biometric characteristics can be divided [3]:

- **Anatomical/Physiological**: these human features are related to the morphology or anatomy of the individual. This can be, for example, the face, fingerprint, iris or the hand geometry, but also include the odor of the person and its DNA.
- **Behavioral**: humans show certain characteristics related to their behavior, generally influenced by their surroundings and not necessarily genetically imposed. Some examples include signature and body motion movements, and they are also denoted as behaviometrics.

When using biometrics as a form of identification, physical characteristics that remain constant and that are difficult to change on purpose are required. What constitutes a good biometric recognition trait depends greatly on the requirements of the application. However, there are a number of requirements that any biometric feature used for identification purposes must satisfy to some extent [17]:

- **Universality**: each person should have the characteristic.
- **Distinctiveness**: how well the biometric separates individuals from each other. Any two persons should be sufficiently different in terms of the characteristic.
- **Permanence**: how well the biometric resists aging and other variance over time.
- **Collectability**: ease of acquisition for measurement.
- **Performance**: refers to the accuracy, speed and robustness of the technology used, as well as the operational and environmental factors that affect them.
- **Circumvention**: resistance to be fooled or copied.
- **Acceptability**: degree of social and personal acceptability.

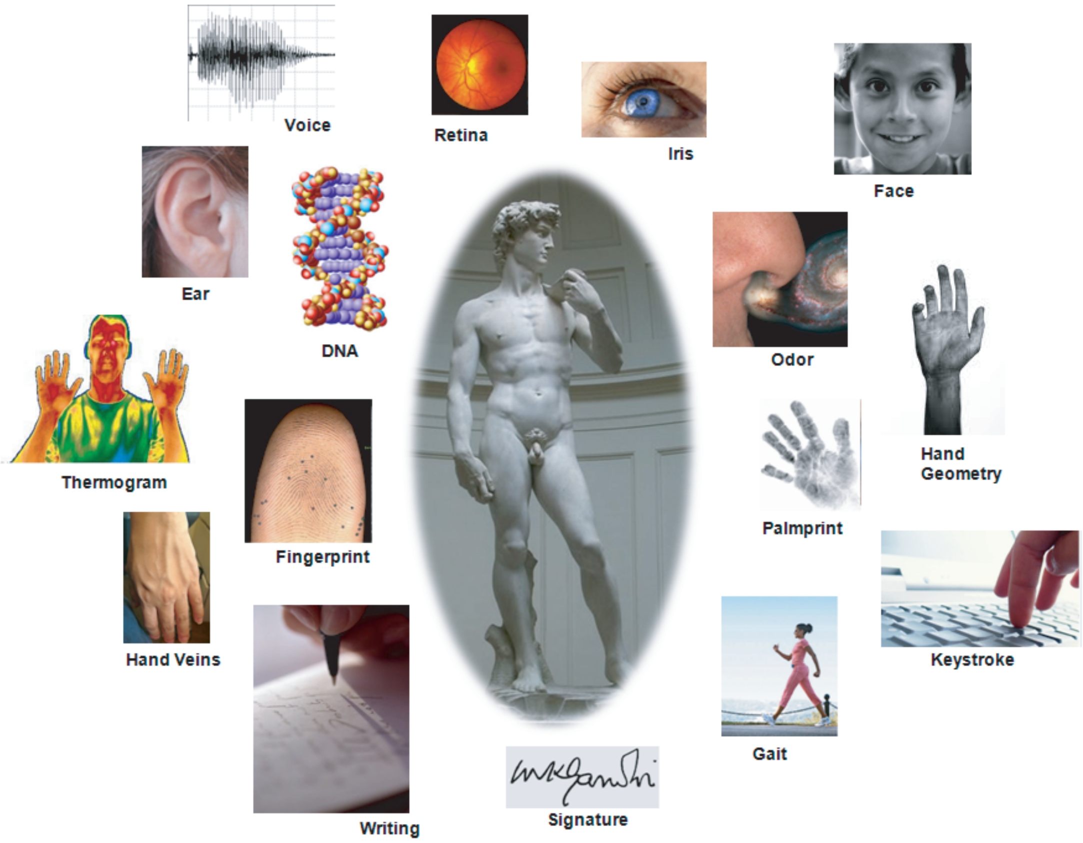
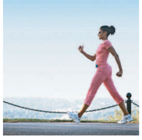


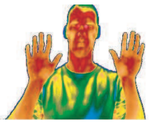
Figure 3.1: Human Biometric Features

3.2. Overview of commonly used biometrics

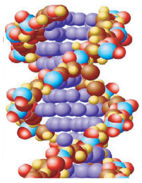
None of the existing biometric features has all the previously mentioned characteristics simultaneously. Some traces perform better than others under certain conditions, but all of them have their weak points and disadvantages. The final use of a certain biometric will be determined by the application. Here, a brief explanation of the most commonly used biometrics is presented. In Table 3.1 one can compare the degree of fulfillment of these requirements for the most commonly used biometrics. An example of the most commonly used biometrics is also found in Figure 3.1.



Gait. Gait is the distinctive way one walks. Despite the complex spatio-temporal scenario it needs to deal with, its acquisition is extremely simple and cheap. It belongs to the behavioral biometrics and it is not supposed to be very distinctive. Also, the lack of secrecy of this biometric (everybody can see how one walks) makes it weaker to impostor attacks (it easier to imitate than a fingerprint pattern). On top of that, gait is something that easily changes over time, due to changes in the body, and it may even vary according to the type of footwear used. However it may be valid as a complementary measure in controlled environments where the user is forced to follow a certain path (for example, in airports). Nevertheless since this technique is based in video-sequences, it is computationally expensive and more research needs to be done in the field.



Infrared Thermogram. The human body releases heat that can be captured with an infrared camera to constitute what it is believed to be a unique pattern for each individual. Different thermograms can be acquired, such as facial, body or hand, in a nonintrusive fashion and with or without the user's cooperation. However, this method becomes impracticable when there are other heat emanating surfaces near the body. The price of infrared sensors has served as tough drawbacks for this technology.

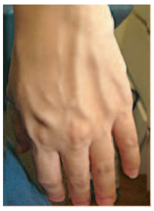


DNA. The DNA (Deoxyribonucleic acid) differs from standard biometric features in that it requires a physical sample rather than an image or recording. Despite the fact that 97 % of all DNA is shared, DNA is actually unique to every individual except for identical twins and does not change during life. It is a commonly used method in forensic applications. However, it presents some serious drawbacks that make it ineligible as a biometric characteristic. The first one is the ease of obtaining a sample (tissue, glass, gum, hair, etc) that make it very vulnerable to robbery and identity impersonation. Also, the DNA extraction method is not immediate since it requires complex chemical methods and currently not all stages of comparison are automated. Finally, the tissue from these DNA samples can not only be used to identify individuals, but it can also be used to produce information in relation to health, paternity and other personal issues, which may lead to genetic discrimination and privacy threats.

Face. The face is a widely accepted biometric since it is the feature that humans intuitively use to distinguish from each other, along with the voice. Face recognition software takes a number of points and measurements, including the distances and angles between key characteristics of a human face, such as eyes, nose and mouth and creates a template including all the numerical data. Current efforts also include the detection of particular features such as wrinkles and furrows. It is considered one of the less intrusive methods and has thus a higher level of user acceptance. Face recognition is also known by its potential to operate at a distance, with or without user cooperation; however, this may lead to security risks, since the face is on public display and can easily be stolen and spoofed. Also, for machine identification it poses more of a technological challenge, currently having lower accuracy rates than the other principal modalities in non-ideal conditions. These systems have difficulties in recognizing faces under different angles and illuminations, not to mention the possible variety of expressions that a person can display through the face.

Ear. It has been suggested that the shape of the ear can be used as a biometric feature. There are several methods that use the distance of salient points of the ear for recognition, although none of them give a reliable performance rate. The image capturing process is much simpler compared to face biometrics: it has a reduced spatial resolution which makes it less variable to pose, illumination or expression. It is also more stable over time than facial structure. However, there are no conclusive proofs that the ears of all people are unique.

Fingerprint. Fingerprints were the first biometric identifiers to be used for law enforcement purposes several centuries ago. They are probably the best known and most extensively used features due to their uniqueness and complexity. Nowadays the ink impressions of the fingertips have been substituted by sensor with automated processes that perform individual identification with high reliability and performance. Fingerprint recognition is based on a pattern of ridges and valleys from which position and orientation of some particular points are extracted. The two main challenges of this technology are the lack of interoperability in a commercial context between systems from different vendors and its non universality (it is estimated that about 5 % of the population do not have a fingerprint suitable for recognition). Also, the variability of this biometric can be high as an individual ages and due to different manual activities.



Hand Vein Structure. Another human structure that is believed to be unique for each individual is the hand vein structure. Using near infrared imaging, one can obtain this veinprint, hard to spoof and forge. Some of the difficulties when working with this technology are the three-dimensional space and orientation of the hand, along with the high price of the sensors needed.

Hand Geometry. Thanks to its simplicity and ease of use, the technology based on the hand geometry has been used since the late 60's, when the first automated biometric systems were installed. The process consisted in a comparative between shape and size of the palm, sizes of fingers and measures of joints to distinguish between individuals. It has a good performance not affected by weather conditions nor individual anomalies. However, hand geometry is not a very distinctive feature and thus it cannot be used on a large population, limiting its use. Also, it is stable only in a limited period of age, since hand geometry varies during the growth period of children and due to deformations on senior citizens.

Palmprint. After the big success of fingerprints as a biometric, palmprints are seen as the next step in biometric security. Just like fingerprints, they provide a unique sequence of ridges and valleys, distinctive for each individual. Although still in development, the larger size is expected to make palmprints more reliable and accurate than fingerprints. The drawbacks of this technique deal with the image capture: the larger area needed to be capture would require a bigger sensor. Recent works require only to position the hand in front of a camera. This has other implications in terms of spatial variability (3D rotation) which needs to be compensated.

Iris. Recognition based on iris is among the most commercialized applications within biometrics, being already in use in high-security applications with very good performance rates. The iris texture is highly distinctive from one person to another, being different even from one eye to another and with the only exception of genetically identical twins. Although it is a non-invasive technique, it requires the user's cooperation. The image must be captured within a few meters but even though it does not require physical contact with the sensor, users have reported discomfort when using the system. New less intrusive methods that can capture iris images from a larger distance are trying to increase the acceptance of the iris modality.

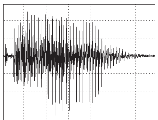
Retina. Retina biometric gives up commodity for security. A retinal scan captures the vascular configuration of the eye, unique for each individual. Its location inside the eye makes of the retina one of the most secure biometrics, being hard to change and replicate. However, it requires cooperation from the subject since it cannot be acquired at a distance, and needs the person to look through a lens. Furthermore, retinal scans can reveal medical conditions, which raise privacy concerns.

Odor. Just like each individual has a different DNA, the chemical composition varies slightly from one to another. This means that each object spreads around a unique odor that can be distinguished from others through a number of chemical sensors. The process is not immediate and other substances such as deodorants and perfumes could decrease the accuracy of this method.

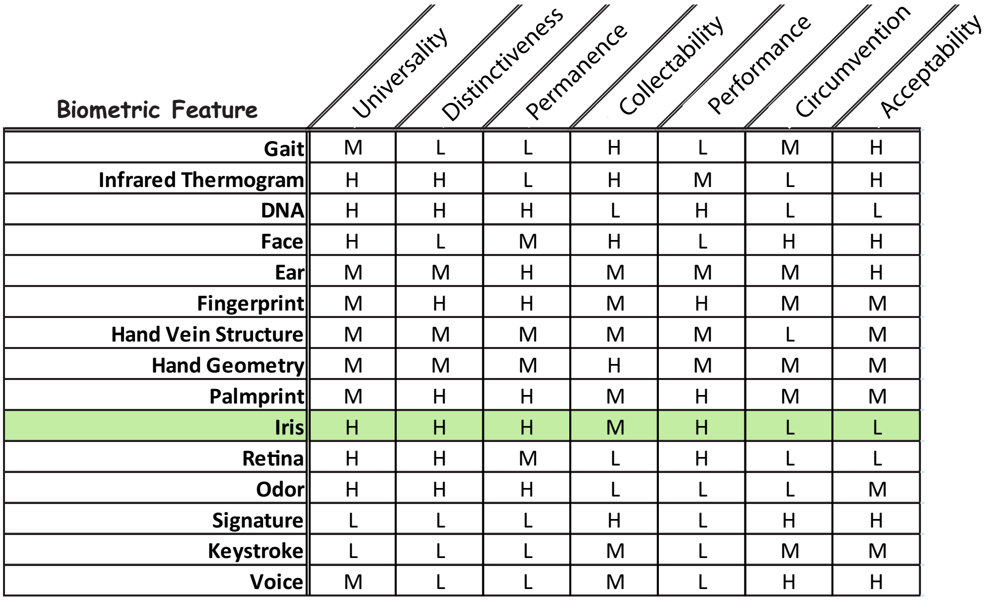
Signature. Signature is a handwritten depiction of someone's name. It has been traditionally accepted to give evidence of identity and is therefore widely accepted among society. However, signature is a behavioral trait so it is subjected to changes over time. Not only in the long term but in each execution the signature may vary, influenced by the pressure and velocity of the pointer across the sensor.

Writing. Writing also belongs to the behavioral biometrics, and therefore it is characterized by its variability over time. Its strongest advantage is the easy of capture. On the other hand, it is necessary a reasonable amount of text to obtain good recognition rates, which can be a problem in some scenarios (e.g. forensic).

Keystroke. Although there are no strong evidences yet, it is believed that keystroke may be characteristic for each individual and can be used for verification. It is very convenient since keystrokes can be monitored non-intrusively. However, as a behavioral biometric, it suffers from large variations even in the same day.



Voice. When using voice as a biometric feature, one can analyze the pitch, tone, cadence and frequency of the person's voice. Strictly speaking, voice is a physiological trait, because every person has a different vocal tract. But voice recognition is also based on the study of the way a person speaks, which is classified as behavioral. Due to its variability over time, voice systems must be heavily trained to form a pattern that can be recognized later on. However, the ease of capture of this biometric through everyday methods such as the telephone for example, makes it feasible for a number of remote applications.



Biometric Feature	Universality	Distinctiveness	Permanence	Collectability	Performance	Circumvention	Acceptability
Gait	M	L	L	H	L	M	H
Infrared Thermogram	H	H	L	H	M	L	H
DNA	H	H	H	L	H	L	L
Face	H	L	M	H	L	H	H
Ear	M	M	H	M	M	M	H
Fingerprint	M	H	H	M	H	M	M
Hand Vein Structure	M	M	M	M	M	L	M
Hand Geometry	M	M	M	H	M	M	M
Palmprint	M	H	H	M	H	M	M
Iris	H	H	H	M	H	L	L
Retina	H	H	M	L	H	L	L
Odor	H	H	H	L	L	L	M
Signature	L	L	L	H	L	H	H
Keystroke	L	L	L	M	L	M	M
Voice	M	L	L	M	L	H	H

Table 3.1: Comparison of characteristics between different biometric features (H=High, M=Medium, L=Low). Based on the perception of the authors of [3].

According to the International Biometric Group [18], the most widely used biometric technology is fingerprint scanning, which accounts for more than 65 % of biometric system sales, and face recognition with a 11 percent of the market, followed by hand geometry, iris recognition, voice scanning and signature scanning. Retinal scanning-which reads the blood vessels in the back of the eye and requires the user to be within six inches of the scanning device-is the most accurate system but also the least likely to enjoy widespread use because of people's natural protectiveness toward their eyes. The distribution of revenues from biometric systems can be seen in Figure 3.18.

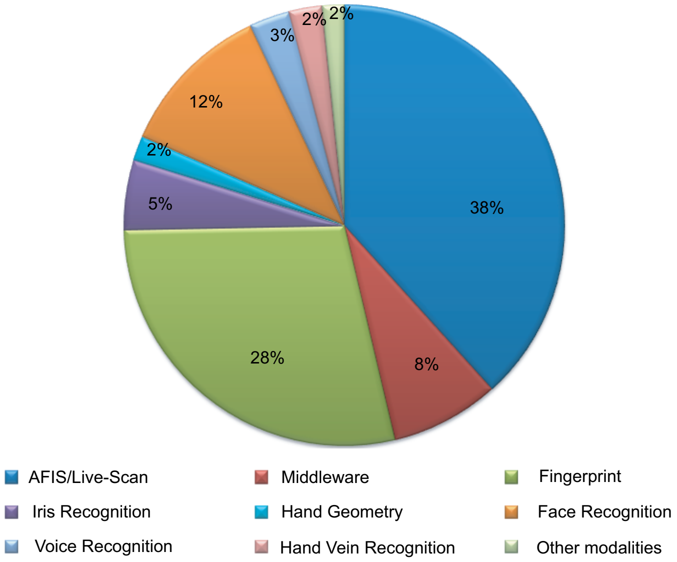


Figure 3.18: Revenues obtained from different segments of the biometrics market.

3.3. Biometric Systems

3.3.1. Basic Working Scheme

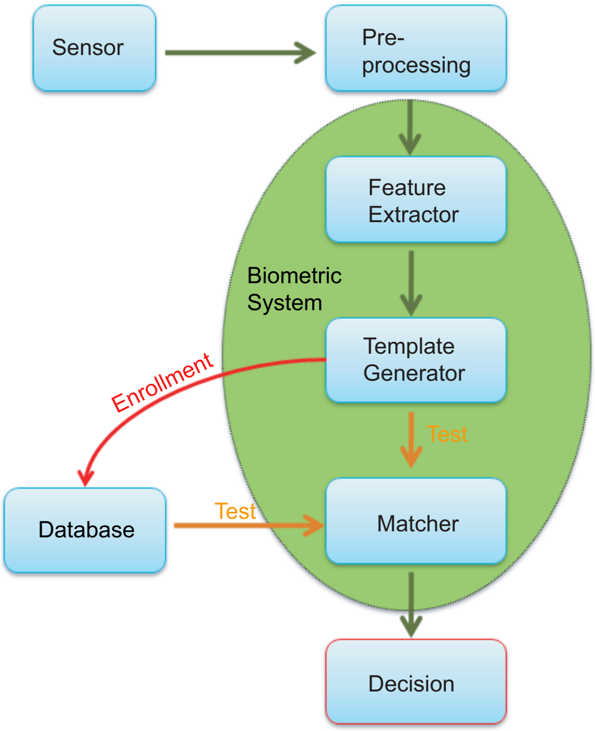


Figure 3.19: General structure of a biometric system.

A biometric system is the combination of devices, databases and processes that allow the recognition of an individual using one of his/her biometric features. Every biometric system shares a number of common modules, although its final configuration will depend on the type of signal or pattern that it will deal with. In Figure 3.19 there is a representation of a biometric system with the basic components highlighted.

In general, a simple biometric system must include four basic components:

- A *sensor* to acquire the biometric data
- A module to perform the *feature extraction process*
- A *matcher* where the previously extracted features are compared with the templates in the database
- A *decision- making component* that will verify or deny that the individual is who he claims to be.

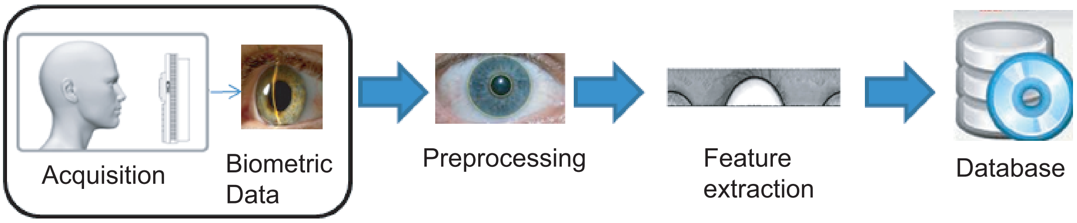


Figure 3.20: Block diagram of biometric recognition systems during the enrollment process.

The first time an individual uses a biometric system it is necessary to store his/her biometric information that will later on be used as reference for comparison. This process is called enrollment (see Figure 3.20) and it represents a crucial step in the system since it needs to provide a safe storage and retrieval of such data. The sensor is responsible for capturing all the necessary analog data and turning it into digital information, since it will be the interface between the real world and the system. Most of the time, an intermediate step is added to pre-process (remove background noise, enhance, normalize, etc.) the captured data. Features are then extracted from the pre-processed information in a second step and stored into templates that will represent the identity of the captured individual. Templates contain less information than the original sample since the data not useful for recognition is discarded. This helps reduce the amount of memory needed, increases the security of the system and speeds up the matching step. When an enrolled individual makes use of the system, the matcher will compare the new captured data with that existing in the database and will assign a certain similarity measure between them, which will assist in the task of recognizing the captured individual. Biometric systems can be used for positive or negative recognition. Positive recognition aims to confirm is a users is truly who he claims to be. Negative recognition tries to determine that a user is who he denies to be (for example, a criminal). This second type appeared with the introduction of biometrics, since it was not possible to carry out with traditional security measures such as keys or passwords.

Based on its application, systems can work on-line or off-line. On-line systems make use of live captured biometric data, and they are completely automatic since they require a fast, almost immediate decision generation, for security purposes like restricted areas access control. Off-line systems on the other hand, do not make use of live captured data, such as the ones used in forensics (e.g. latent fingerprints or handwritten documents obtained from criminal investigations). Due to their nature, these systems necessarily have to allow a certain delay in the recognition process. This delay introduces the possibility of human supervision, which generally implies an improvement in the results. In the case of forensic identification, the process can return a list of possible candidates that will then be supervised by an expert.

3.3.2. Operational Modes

Once the users have been enrolled, biometric systems can operate in two modes:

- **Verification** (Fig. 3.21): a one to one comparison of a captured template with only those templates corresponding to a previously claimed identity is done. The system will compute the similarity degree between the captured template and the claimed identity, resulting in an acceptance or rejection decision.

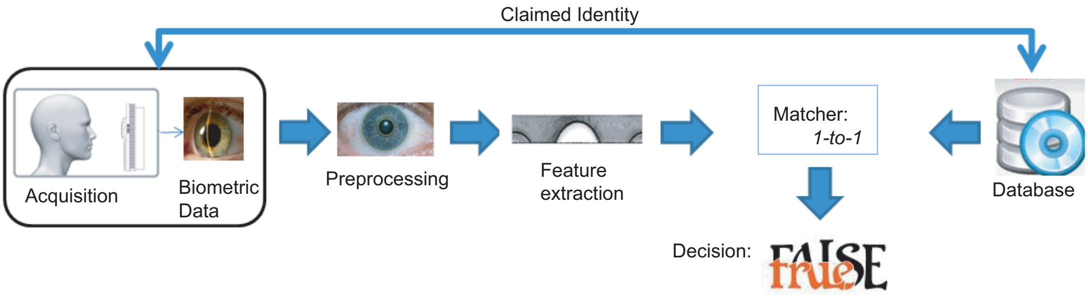


Figure 3.21: Block diagram of a biometric recognition system in verification mode.

- **Identification** (Fig. 3.22): a one-to-many comparison of the captured template against all the users in the database is done, outputting the identity of the user which is most similar to the captured template. Ideally, the first ranked candidate (Top 1) should correspond with the correct identity of the individual, but one can choose to consider a longer output list (e.g. Top 10) to increase the chances of finding the correct identity. A special application of identification, known as screening, is used to determine if a person belongs to a list of wanted identities. Mainly used in security applications such as airports or terrorists identification, people to be identified have generally not chosen to be in those databases.

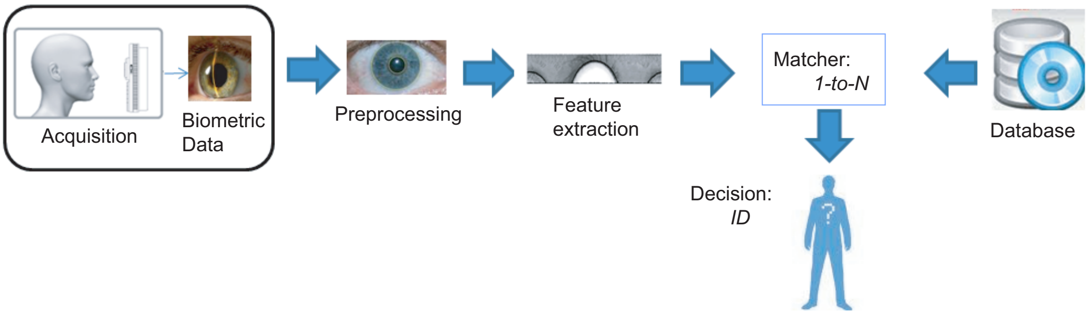


Figure 3.22: Block diagram of a biometric recognition system in identification mode.

3.3.3. Performance Evaluation

When a biometric system is implemented, an objective and quantitative measure is needed to compare its performance with that of already existing methods. This measure will also help the developer to evaluate and improve the system.

Two samples of the same biometric trait will have small variations due to different acquisition techniques, the interaction of the user with the sensor, environment conditions or changes in the individual itself. Therefore, the matcher of a biometric system will return a similarity measure or score that quantifies the similarity between the input sample and the pattern stored in the database. The more similarity between samples, the higher score the matcher will return, which means that the certainty that both samples belong to the same individual is high. Final decision will be controlled by a threshold: input samples will be assigned to an individual's identity if their score exceed the threshold value. This value will be influenced by the level of security that the application requires, which is analyzed next.

When working in the *verification mode*, two main metrics are used to measure the performance of biometric systems:

- **False Accept Rate (FAR) or False Match Rate (FMR)**: when working properly, biometric devices are much more reliable than password based security. However, there is always the possibility that a biometric system will incorrectly match the input sample to a claimed identity stored in the database. The probability that this happens is known as FAR (or FMR). These false positives can be due to failures in the hardware (cheap sensors) or holes in deployed software. Because a non authorized person accepted as authorized can often lead to damages, FAR is a relevant security measure.

- **False Reject Rate (FRR) or False Non-Match Rate (FNMR)**: The FRR or FNMR reflects the probability that a genuine score falls below the decision threshold and is rejected by the system. This is, a valid input that is incorrectly rejected as not corresponding to the claimed identity. FRR is thought as a comfort criteria, since the rejection of an authorized person is most of all annoying.

These error rates come in pairs; for each false-reject rate, there is a corresponding false acceptance. In a perfect biometric system, both error rates would be zero (see Figure 3.23 (a)). Unfortunately, variability of biometric systems makes necessary the imposition of a trade-off. The denial of access to all individuals by using a very high threshold would lead to a false-reject rate of 100 % but a false-acceptance rate of zero. At the other extreme, by granting access to everyone by using a very low threshold, the FRR will be zero but the FAR will be 100 %.

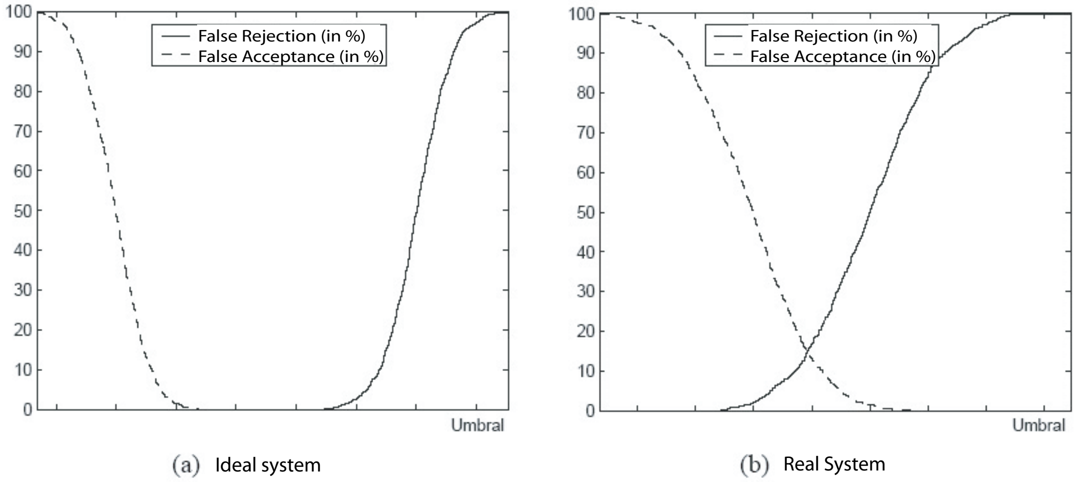


Figure 3.23: FAR and FRR curves.

Biometric systems operate between these two extremes (see Figure 3.23 (b)), resulting in a compromise between the FAR and the FRR.

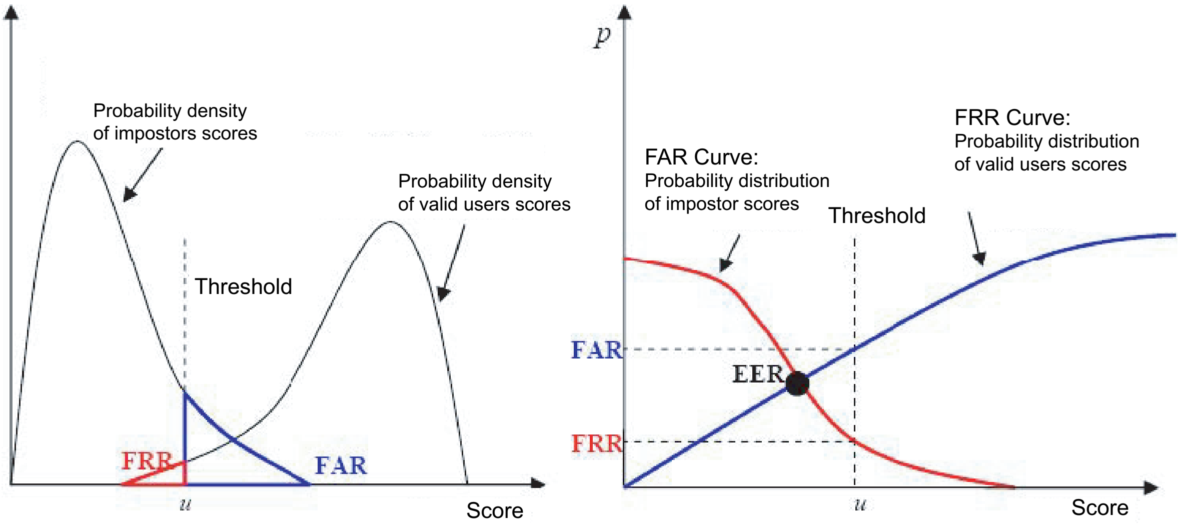


Figure 3.24: Probability densities and distributions of users and impostors.

The performance of a biometric system can be characterized by a single measure known as Equal Error Rate (ERR). This is the intersection point between the FAR and FRR curves, and therefore, the rate at which both accept and reject errors are equal. It measures the degree of overlapping between the FAR and the FRR distributions. From Figure 3.24 it can be observed that the lower the ERR, the more accurate the system is.

However, the ERR is not necessarily the optimum working point. The relationship between the FRR and FAR can be represented as a single curve known as Detection Error Trade-off (DET), which plots the FAR vs. the FRR for all the different threshold values (see Figure 1.26). For good systems, the DET curve lies very near the origin. DET measures allow a comparison between different systems independently of threshold parameters.

When working in the *identification mode*, the system must compare the captured input data with all the identity models stored in the database. If the most similar model corresponds to the input identity, then a successful identification is claimed. For this mode, the error measure is computed as the rate of correctly identified users.

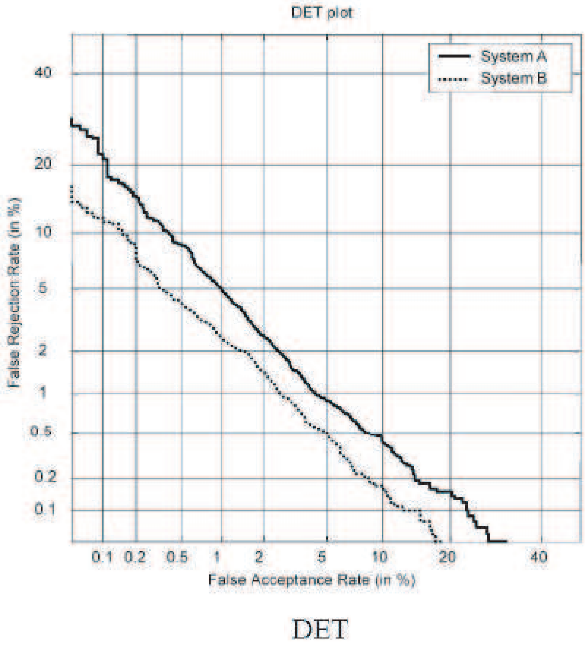


Figure 3.25: DET Curve.

3.3.4. Applications of Biometric Systems.

Biometrics is being increasingly used in a number of applications due to its practical advantages over traditional recognition methods. These applications can be grouped in three main groups:

- **Forensic Applications**: Forensic is the original application in which human features, such as fingerprints, were used for identification. For a long time, experts in the field have matched manually these features for recognition and classification. Nowadays, automatic processes allow significant time savings and make applications such as corpse identification, criminal investigation, terrorist identification and so on much more reliable and accurate.
- **Government Applications**: The government sector represents a large market for biometric applications. It includes ID card programs, benefits program fraud prevention, background checks, logical and physical authentication, passenger screening and visitor tracking. Traditionally this sector has used token-based systems, such as badges and ID cards. The improvements and reliability of biometrics are driving the change with an increasing number of public applications making use of biometrics.
- **Commercial Applications**: A host of networking-associated companies has recently added biometric authentication features to their products, bringing the technique out into the market. Applications such as computer network login, e-commerce, physical access control, ATM or Internet access are switching from the traditional knowledge-based systems, such as passwords or PINs, to new biometric methods that can be deployed for a large-scale population.

Although biometric technologies are still more popular in fiction than reality, there are a number of countries strongly advocating for this technology. USA, Brazil, Iraq, and Australia, along with many other European Countries, are some of the nations including biometrics in their security systems. Examples include from iris scanning in airport controls (e.g. Amsterdam, Heathrow) to fingerprint lockers in theme-parks of the US.

3.3.5. Limitations of Biometrics Systems

- **Performance**: Some biometric traits are known to be more accurate than others, but there is an intrinsic upper-bound in the performance that any biometric trait can provide. The inaccuracy of biometric systems is related to the statistical nature of the acquisition and matching stages. Unlike password-based systems, biometrics does not look for a perfect match between two strings in order to identify a user, but for a feature vector that matches a certain percentage above a certain threshold. As a result, there is always the possibility that a biometric system will incorrectly match the input identity with one stored in the database (i.e., a false match) or incorrectly reject a valid input identity (i.e., a false non-match).

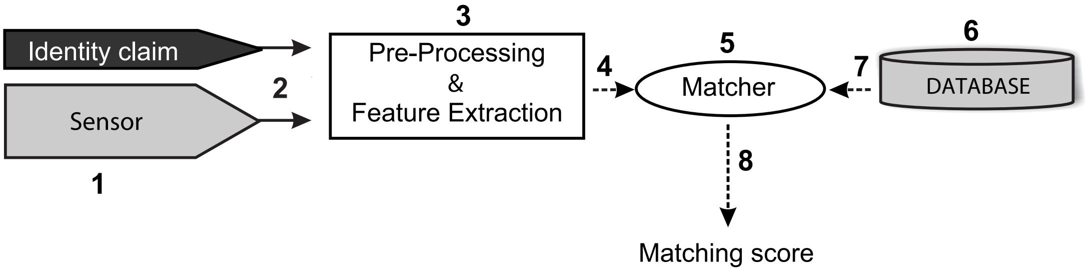


Figure 3.26: Points of attack to biometric systems.

- **Security**: Biometric systems only represent a secure identification process in as much as they provide a reliable relation between physical individuals with their identity information. The main drawbacks of biometrics are the lack of secrecy (everyone knows our face or could get our fingerprints) and the fact that, unlike passwords that can be reset, a biometric trait cannot be replaced. Therefore it is necessary to remember that biometric systems are vulnerable and can be "spoofed". In [6], Ratha et al. identified and classified eight possible attack points to biometric recognition systems. These vulnerability points, depicted in Figure 3.26, can be divided in two groups:
  - **Direct attacks**: The system is stroked through the sensor (point 1 in Figure 3.26) using synthetic biometric samples. This type of attack does not require previous knowledge of the system since it happens outside of its physical limits, although in principle it will not be effective in supervised systems.
  - **Indirect attacks**: The remaining points in Figure 3.26 are grouped under this type. Attacks 3 and 5 might be carried out using a Trojan Horse that bypasses the system modules. Points 2,4,7 and 8 represent weak points in the communication channels of the system and attacks in point 6 correspond to manipulations of the database. These vulnerabilities require physical access to the system and previous knowledge of its configuration. Attacks can be performed using for example hill climbing techniques, introduced in [19].
- **Inconsistencies**: Biometric templates stability greatly depends on the method and environment of acquisition, and the interaction of the user with the system. Variations in the representation of the biometric features can lead to inconsistencies with the database and an increase of the FRR. The main reasons for these variations are [4]:
  - **Inconsistent presentation** (Fig. 3.27): When the sensor characteristics are varied or the interaction with the device is incorrect, the biometric data acquired during authentication may be very different from the one stored in the database during enrollment. For example, the orientation of a face in front of the camera or the mapping of a tridimensional finger onto a two-dimension sensor can create inconsistencies that affect the recognition process.

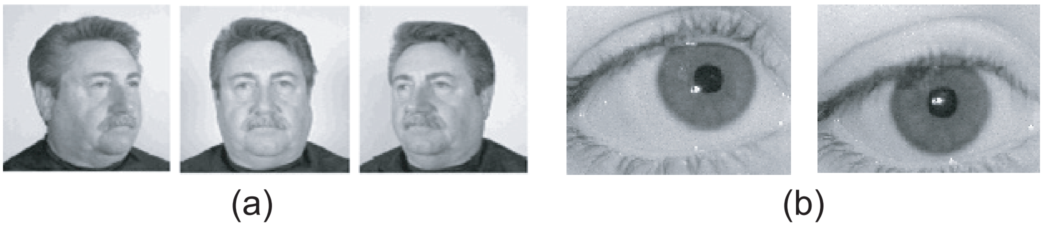


Figure 3.27: Inconsistent presentation. Variations of a biometric signal: (a) Face orientation (b) Iris position.

- **Invalid acquisition** (Fig. 3.28): The environment conditions in which an acquisition takes place have a great effect in the identification process. Light, channel characteristics or non-uniform contact with the sensor are some of the characteristics that produce variations in the captured signal. For example, the accumulation of dirt in the sensor can determine an invalid feature vector.

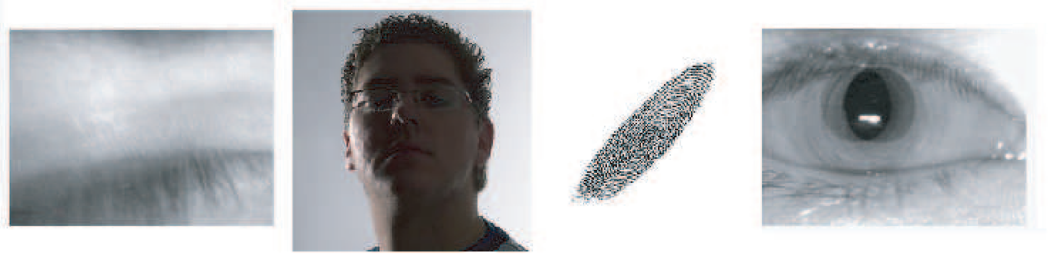


Figure 3.28: Invalid acquisition. Imperfect captures of iris, face and fingerprint features.

- **Non-reproducible data** (Fig. 3.29): A captured biometric can be distorted by many different sources. A scar in a fingerprint, sunglasses on a face or a ring on a finger can produce noise enough during the acquisition process that the system cannot perform identification. Some of the variables can be discarded by with supervision of the system, but some are permanent and non-reversible (serious burns or amputations).

Figure 3.29: Non-reproducible data. Variations of biometrical data due to external agents.

- **Other limitations of the biometric systems**: Biometric systems are not only affected by error rates and limitations of the features, but also by the usability of the systems. There are a number of issues that need to be addressed since they play an equal role in determining the effectiveness of these systems. The most important include the non-universality of a biometric trait and its distinctiveness. Although every user is expected to possess the biometric trait being acquired, there might be a percentage of the population who do not have it. This creates a failure to enroll that for the case of fingerprints it has been estimated to be of 4 % [3]. Also, biometric data is subject to changes and evolution across time, so data acquired at two different moments may be very different, reducing its power of discrimination. A possible solution for this issue is to use a multimodal biometric system (see Sec. 3.5) to make identification more robust and accurate.

3.4. Social Aspects and Privacy

Biometric technologies try to increase security by not storing raw biometric data but only a vector containing the most relevant features useful for recognition. However, the stored data can be linked to other existing information about the individual that can result in an invasion of privacy. Despite the existence of a legal framework for Data Protection, the diffusion of biometrics into the commercial world is not well received by many users. Although people are used to having a picture taken of their faces, they are not very willing to share the retina pattern, as it requires an inconvenient acquisition method. This gives a sense of the importance of creating a user friendly environment: features that can be acquired without cooperation enjoy the approval of the users. However, too little or “none required” cooperation are normally regarded as threats toward privacy and consistently lead to suspicions. Therefore, it is very important to establish a clear purpose of the application for which the system will be used. Human factors such as age, ethnicity, gender, diseases or disabilities should be excluded from the identification process or their impact minimized to avoid the exclusion of part of the population.

Some of the ideas currently under research include the use of non- reversible transformation of the extracted feature vector to avoid reverse engineering and the implementation of data protection and encryption measures. The combination of multiple biometrics or the use of smart cards are other possibilities that may help overcome the barriers that biometrics encounter in society. In the latter case, biometric data is stored in a smart card that is carried by the user, avoiding biometric data to travel across data networks or to be stored in external databases.

3.5. Multimodal Biometric Systems

Some of the problems introduced for the unimodal biometric systems can be solved by using multiple evidences of a person’s identity. These systems are known as multimodal biometric systems and they use more than one physiological or behavioral characteristic for recognition. The main benefit of multimodality is an increased accuracy and security against spoofing attacks.

Multimodal systems can refer to their multiplicity in different aspects (see Figure 3.30). The most common scenarios are [3]:

1. **Multiple sensors**: The same biometric trait is captured with different biometric sensors, and the information of all of them is then combined. For example, in fingerprint acquisition, features can be obtained with optic sensors, 3D sensors or solid state sensors [17].

2. **Multiple biometric traits**: Recognition is based on multiple biometric traits of an individual, such as face and fingerprint. The independence between each source improves the robustness of the system. The more biometrics used the more certain the decision of identification will be. An example of the use of multiple biometric traits is shown in Figure 3.31.

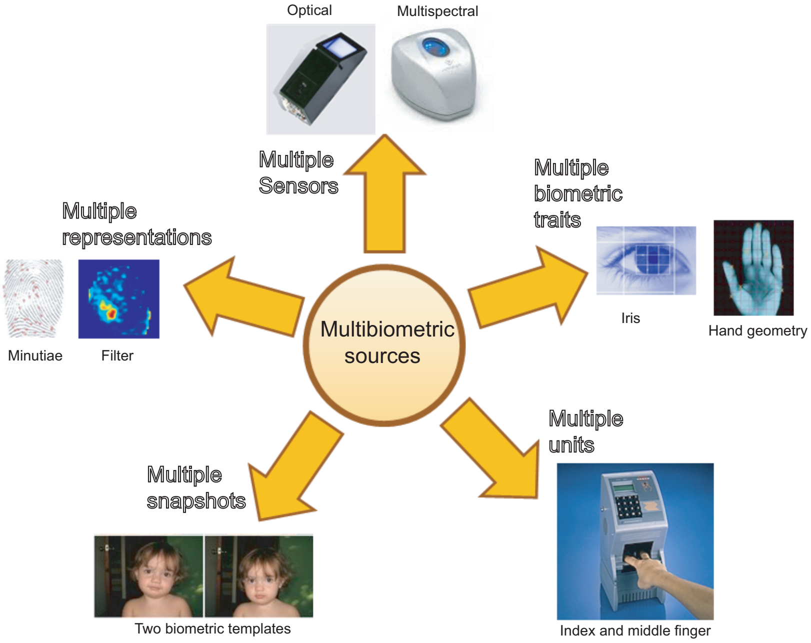


Figure 3.30: Various scenarios in a multimodal biometric system.

3. **Multiple units**: Humans have a few "repeated" biometric features, such as eyes, fingers or hands. Recognition is done in this case by combining the information presented by two or more fingers (or irises, hands. . .).

4. **Multiple snapshots**: The combination of the information acquired by multiple acquisitions of the same biometric feature can result in a more complete and accurate description of the individual. Several voice samples of multiple face images would be an example of biometric multiplicity.

5. **Multiple representations**: A single biometric trait is analyzed with several feature extractors, all of them working with the same raw data but processing it differently. Therefore, each of them generates their own features, which can be matched separately. Then, the matching scores obtained from the different classifiers can be combined to make a decision.

Figure 3.31: Capturing face, voice and fingerprint biometric data.

In addition, a multimodal system can operate in three different modes when combining information from different sources:

- **Serial mode**: the output of the analysis of a biometric source is used as the input for the next one, narrowing down the number of possible identities in each step. This means that not all traits have to be acquired simultaneously and a decision can be made before all the features have been captured if enough certainty is achieved. A useful configuration for this operational mode is to start with a fast although less accurate recognition system that reduces the number of comparisons to be done subsequently by slower but more precise systems.

- **Parallel mode**: the decision is based on the information of all the captured biometric features. This means that all the acquisitions must be performed before the process can conclude. This mode is very robust, especially for identification purposes.
- **Hierarchical mode**: individual classifiers are combined in a treelike structure. This scheme combines the advantages of both previous methods, and it has special relevance when the number of classifiers is large.

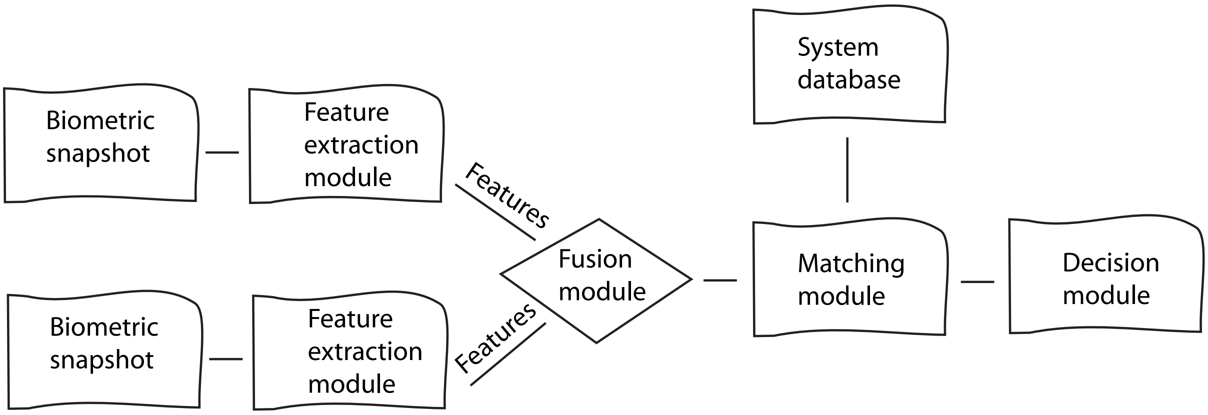


Figure 3.32: Fusion of information at the feature extraction level.

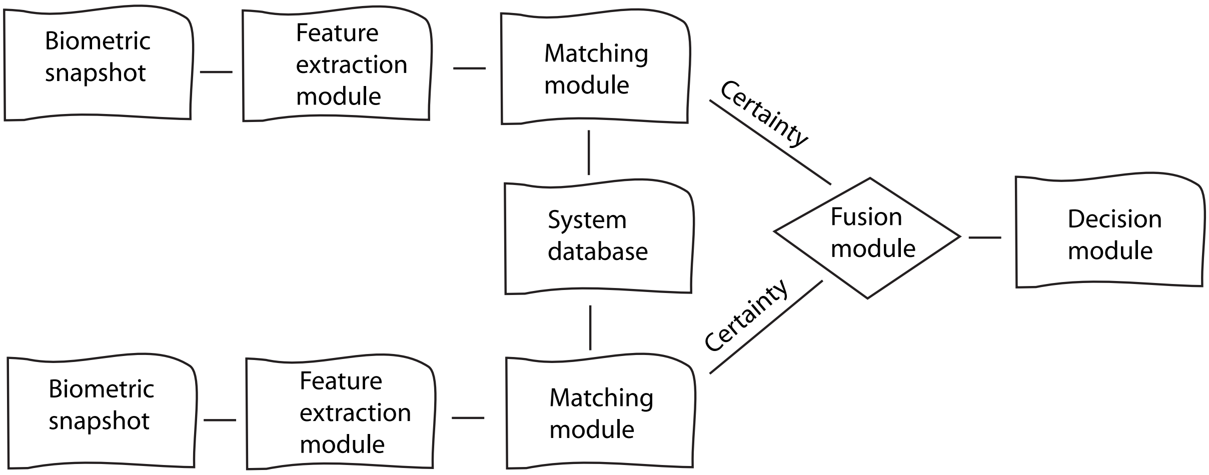


Figure 3.33: Fusion of information at the score level.

Finally, multimodal biometric systems offer different levels for the combination of the information of the different individual characteristics. One of them is the combination at the *feature extraction level*, which combines the different extracted characteristics. The basic configuration of these systems is presented in Figure 3.32. Characteristics can also be combined at the *score level*, where the different similarity measures obtained from unimodal systems are combined in a single measure, for example by using the mean. The basic configuration of these systems is presented in Figure 3.33. Finally, different decisions of acceptance or rejection can be registered to provide a final decision at the *decision level*, for example using the majority rule. The basic configuration of these systems is presented in Figure 3.34.

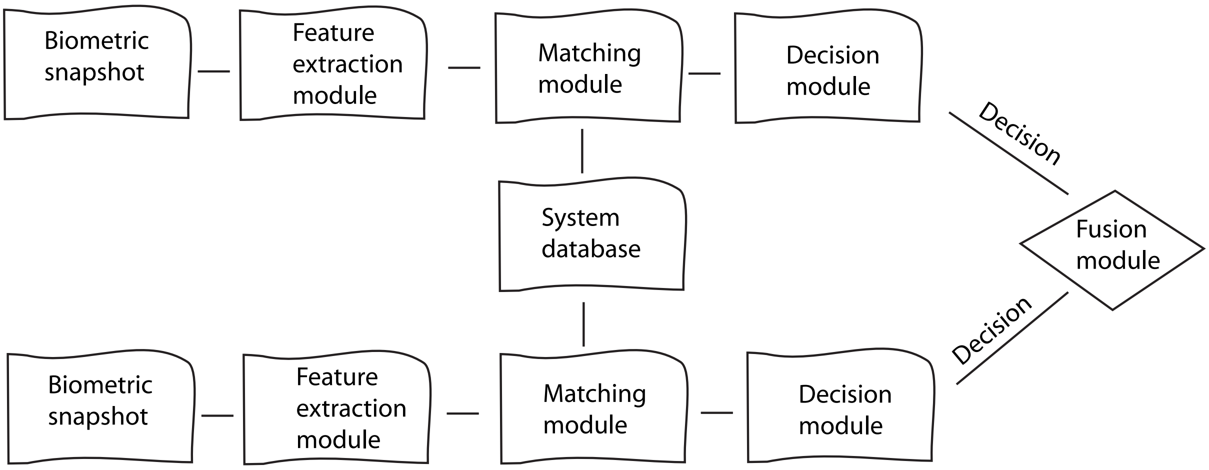


Figure 3.34: Fusion of information at the decision level.

4

Iris Recognition. State of the Art

4.1. Introduction

Biometrics use both anatomical and behavioral characteristics to perform individual recognition. One of the human features that have attracted most of the researcher's attention is the eye. Two different eye-based techniques have been deployed, both grouped under the eye biometrics set: retinal recognition uses the unique pattern of blood vessels on an individual's retina at the back of the eye (*retina-scan*), whereas iris recognition analyzes the features that exist in the iris muscle, the colored tissue surrounding the pupil of an individual's eye (*iris-scan*). Both techniques involve capturing a high quality picture of the iris or retina using a digital camera. However, these are very distinctive methods that only share the same organ, the human eye, as a common characteristic. Therefore it is important to avoid mixing them up by stressing out that the biometric systems which use irides are completely different from those which apply retina patterns in many aspects, from the image acquisition techniques to the feature extraction and the matching methods.

In the current work, a study of the prevalent ocular-based technology, iris recognition, is presented. This research is motivated by the increasing demands of systems that allow automatic recognition based of some sort of unique feature or characteristic possessed by the individual. The uniqueness of eyes, even between the left and right eye of the same person, makes iris scanning very powerful for identification purposes [9]. The iris texture is randomly generated during embryonic gestation, which makes it even more exclusive than the "genetic fingerprinting" (DNA), which is not unique for the about 0.2 % of the human population who have a genetically identical twin [4]. Because of its speed of comparison, iris recognition is a biometric technology well-suited for *one-to-many* identification. Among many others, one of the key advantages of iris recognition is its stability or template longevity over a person's lifetime. The iris is an internal organ that is well protected against damage and wear by a highly transparent membrane named cornea. While there are some medical and surgical procedures that can affect the color and overall shape of the iris, the fine texture remains remarkably stable over many decades. Barring a trauma, a single enrollment in the system can last a lifetime (some iris identifications have succeeded over a period of about 30 years). This distinguishes it from other biometric features such as fingerprints, which can be difficult to recognize after years of certain types of manual labor. Furthermore, the iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles that control the diameter of the pupil. This makes the iris shape far more predictable than, for example, face biometrics, which depend on the angle, position and anatomical characteristics of the person. For all of these reasons, iris patterns become interesting as an alternative approach to reliable visual recognition of persons, especially when there is a need to search very large databases.

However, iris recognition needs to deal with some inconveniences. The iris is small and sometimes partly occluded by the eyelid and eyelashes. Therefore, most of the traditional iris recognition systems require careful cooperation by the user and require the user's eye to be within about 25cm of the camera. Yet, several academic institutions and biometric vendors are developing products that claim to be able to capture a person's iris from a distance of up to 10 meters with minimal user cooperation [20]. It also takes up a bit more memory for the data to be stored, but with the advances in technology, this is unlikely to cause any major difficulty. Finally, iris scanning is a relatively new technology and encounters a serious rate of adoption, since many public and private sectors have made substantial investments toward fingerprint recognition. Efforts must then be focused on proving the higher performance and reliability of iris-based recognition systems in order to develop its use in the society.

4.2. History and development.

The idea of using iris patterns for personal identification is over one hundred years old, when Bertillon designed a system based on 9 anthropometric measurements, including the iris, to distinguish between two distinct people [21]. However, it wasn't until 1936 when the ophthalmologist Frank Burch proposed the first automated iris-recognition. By the 1980's the idea had appeared in several films, such as "James Bond" or "Mission Impossible", but it still remained science fiction and conjecture. In 1985 two other ophthalmologists, Aran Safir and Leonard Flom followed Burch's idea and proposed the concept that even genetically identical individuals have completely independent iris textures, and were awarded a patent for the iris identification concept in 1987 [1]. In 1989, Dr. Flom approached Dr. John Daughman, then teaching at Harvard University, to develop an algorithm to automate the identification of the human iris [22]. In 1993, the Defense Nuclear Agency began work to test and deliver a prototype unit, which was successfully completed by 1995 due to the combined efforts of Drs. Flom, Safir, and Daugman. In 1994, Dr. Daugman was awarded a patent for his automated iris recognition algorithms [23], which are the basis for most of the current iris recognition systems and products available commercially. A year later, in 1995, the first commercial products became available. Dr. Flom, Dr. Safir and Dr. Daugman founded IrisSan Corp., the company which held the patent and licensed it. The first specific iris-acquisition camera was introduced in the market by Sensar Corp., first used to capture iris images in automatic cash dispensers. The world's economic situation led to the fusion of both these companies into what is now Iridian technologies, owner of the patents and algorithms and primary promoter of the development of iris-based products and systems. Another pioneer, Richard P. Wildes, was assigned another patent in 1996 for a non-invasive automatic iris recognition system [24]. In 2005, the broad patent covering the basic concept of iris recognition expired, providing market opportunities for other companies that have developed their own algorithms for iris recognition. With the expiration of the patent, and the availability of new datasets and benchmarks, research activity has greatly increased in recent years [9, 25]. The patent on the IrisCodes implementation of iris recognition developed by Dr. Daugman will not expire until 2011.

As for the commercial implementation of iris systems is concerned, law enforcement agencies in the United States began using iris recognition in 1994 when the Lancaster Country Prison in Pennsylvania became the first correctional facility to employ the technology for prisoner identification. The Flughafen Frankfort Airport in Germany allows frequent passengers to register their iris scans in an effort to streamline boarding procedures, an approach also followed by airports in the UK, the UAE and other countries. There is discussion that banks may someday make iris scans a routine part of ATM transactions and some have begun taking the first steps in testing out these systems. The power of this biometric may make it rival fingerprints for booking situations where identification and verification are vital. As it can be seen, iris recognition is a relatively new technology of barely 2 decades old, but all its characteristics as a reliable and accurate recognition system makes it very distinctive among other biometric features [9].

4.3. The human eye

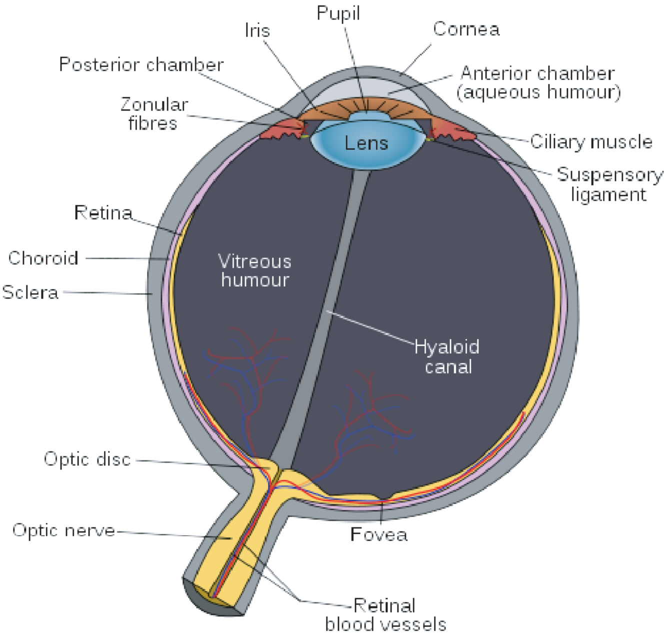


Figure 4.1: Anatomy of a human eye

The visual system allows the assimilation of information from the environment. The eye is an organ which reacts to light and allows vision. About 97 % of the animals known have eyes. The eyes found in different species are different from each other. There are ten different kinds of eyes known, from the simpler structures found in unicellular organism, which do nothing but detect light or darkness, to more complex ones found in humans and other mammals, which give full sense of vision (including color, motion and texture). To avoid misleading, it is important to emphasize that vision occurs in the brain, rather than the eyes. The eye is simply a photoreceptor that converts the light into electro-chemical impulses in neurons.

The human eye allows conscious light perception and vision including color differentiation and the perception of depth. Although the coloration and structure of the iris is genetically linked, the details of the patterns are not. The iris begins to form in the third month of gestation, though a process of tight forming and folding of the tissue membrane. Prior to birth, degeneration occurs, resulting in the pupil opening and the random, unique patterns of the iris. The structures creating its pattern are largely complete by the eight month, although pigment accretion can continue into the first postnatal years. This is why, although genetically identical, an individual's iris is unique and distinct.

The eyeball (see Figure 4.1) is a spherical layered structure of about 2.5 cm of diameter, made of three coats transparent structures. The outermost layer of the three is known as the corneosclera, which encloses and protects the inner eyeball. The uvea is the vascular middle layer of the eye constituting the iris, ciliary body and choroid. The innermost layer situated in the back of the eye is known as retina, which is the light sensitive tissue.

- **Corneosclera.**

The corneosclera, or sometimes simply the sclera, is the term used to define the white part of the eye. It is the outermost layer of the eyeball and it forms the posterior five-sixths of the connective tissue coat of the globe. This layer is made of tough fibers, protecting the eye from penetration of sharp objects. It can be divided in two distinctive although continuous sections: the smaller frontal unit, more curved, called the cornea, which is linked to the larger part called the sclera, which continues up to the dura mater, the outermost of the three layers surrounding the brain.

The sclera maintains the shape of the globe and provides an attachment for muscles, nerves and vessels insertions. The cornea is a strong tissue situate in the front part of the eye that contributes most of the eye's focusing power. It is composed of five layers that allow the light penetration into the inner eye. Behind the cornea there is the anterior chamber, which holds the aqueous humour that separates it from the iris. Transparency, avascularity, the presence of immature resident immune cells and immunologic privilege are some of the more important characteristics of the cornea.

- **Uvea.**

This is the pigmented middle zone of the three concentric layers that make up an eye. Based on their different structures, the middle layer of the eye can be divided into three regions.

The choroid or choroidea is the vascular layer containing the connective tissue of the eye and the provider of oxygen and nourishment to the outer layers of the retina. It is a dark unreflective layer that avoids the light from bouncing all around inside the eye.

The ciliary body is the circumferential tissue that covers from the choroid to the retina. The inner layer is transparent and covers the vitreous body. The vitreous body contains a transparent substance involved in waste management of these areas and nutrient provision, known as vitreous humour. The vitreous body is located posterior to the lens, a transparent, biconvex structure that helps to refract light to be focused on the retina. By changing shape, the lens functions to change the focal distance of the eye, so that it can focus on objects at various distances. The muscles that make this change of shape possible are the ciliary muscles attached to the lens, which constitute the cells of the dilator muscle.

Anterior to the lens is the iris, which regulates the amount of light entering into the eye.

- **Retina.**

Located at the back of the eye, after the vitreous humour, the retina is a complex layered light sensitive tissue, containing the light and color receptors (Figure 4.2). It collects light data and sends it to the brain via the optic nerve. The only neurons that are directly sensitive to light are the photoreceptor cells, which are located on the exterior surface. There are two types: the rods and cones, given this name due to their shape as shown in Figure 4.3 *left*. Rods function mainly in dim light and provide black and white vision. They are a little narrower than cones and with a much greater sensitivity to light, so they require less light to function. On the other hand, this sensitivity to light makes rod cells respond more slowly to light than cones do. Cone cells are shorter than rods, but wider. They are much less numerous than rods in most part of the retina but in the fovea, where they greatly outnumber rods (see Figure 4.3 *right*) . Cones support daytime vision and the perception of color. Since any color of light can be made out of red, green, and blue, it only makes sense that cones are made up of three more light receptors, one for each primary light color. However, they both have the same structural basis. Some real images of cones and rods can be seen in Figure 4.4. Multiple rods cells converge on a single interneuron, collecting and amplifying the signals. However, this union reduces the image resolution, since the combined information from multiple cells is less distinct than it would be if the brain received the information from each rod separately. The convergence of this information also makes peripheral vision very sensitive to movement, and it is also responsible for the vision out of the "corner of the eye". By contrary, each cone cell is connected with a unique nerve fiber, therefore sending the light information individually, with improves the image details.

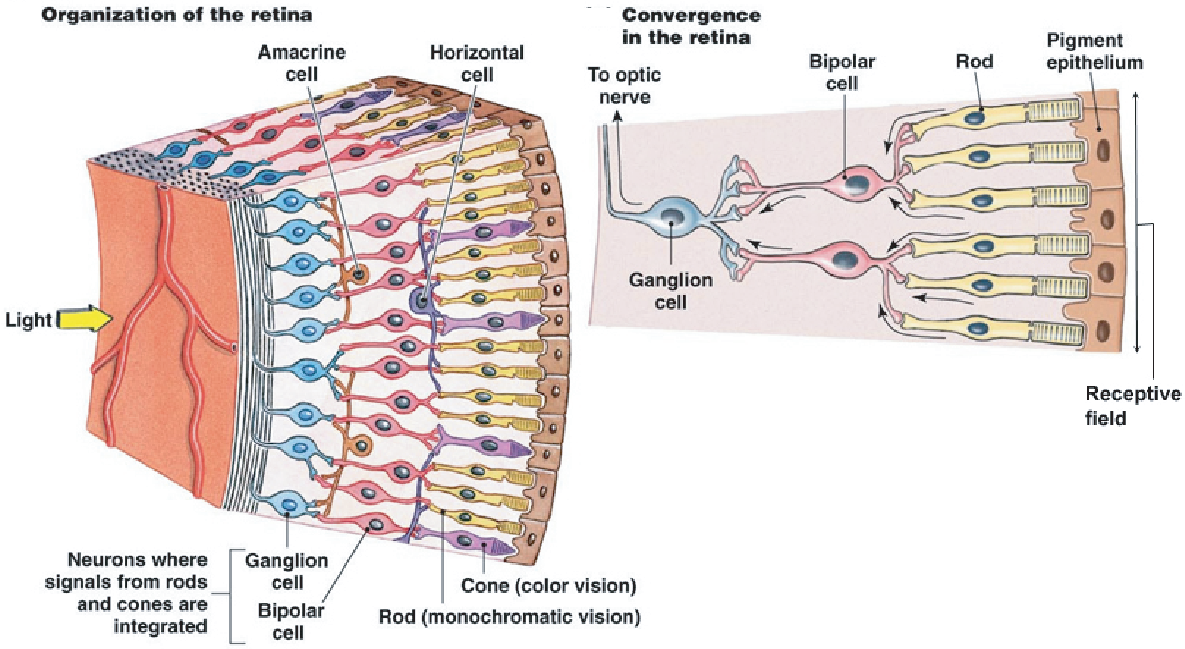


Figure 4.2: Retina structure

The retina also contains the macula, an oval-shaped highly pigmented yellow spot near its center. Light narrows to a point on the macula, which is the center of vision, with the help of the focusing lens. In the center of the macula, there is a point called the fovea, where there are only cones. The fovea is the absolute center of vision. Since the fovea provides the sharpest and most detailed information, the eyeball is continuously moving, so that light from the object of primary interest falls on this region. Because the macula is yellow in color it absorbs excess blue and ultraviolet light that enter the eye, and acts as a natural sun block or sunglasses for this area of the retina. The portion of the electromagnetic spectrum that is visible to the human eye is known as visible spectrum. A typical human eye will respond to wavelengths from about 390 to 750 nm. The distribution of the eye sensitivity to the different wavelengths has a bell, with a maximum value around 600 nm for the cones and 500nm for the rods.

The optic nerve is the cable of nerve fibers with carries the electrical signals from the retina to the brain for processing. The point of departure of that optic nerve through the retina does not have any rods or cones, and thus produces a “blind spot”.

4.3.1. Special considerations of the iris

A little more deeply, the iris is a thin, circular structure in the eye, responsible for controlling the diameter and size of a circular aperture located close to its center known as pupil, which is in charge of regulating the amount of light reaching the retina. It lies between the cornea and the lens of the human eye, and it consists of a number of layers with dense pigmentation cells. The color of the iris is what we know as the “eye color”, which can be green, blue or brown. The externally visible surface is divided from the inner papillary zone by the collarette, which appears as a zigzag pattern.

Being an externally visible, yet protected organ whose unique pattern remains stable throughout adult life [3], iris recognition becomes a very attractive technique for biometric identification. Genetics determine only the general structure, but the color and size of the pupil that gives the detail are generated randomly during gestation, making it a very unique human feature. The only modification that the iris suffers throughout an individual’s life is in its color. Although eye

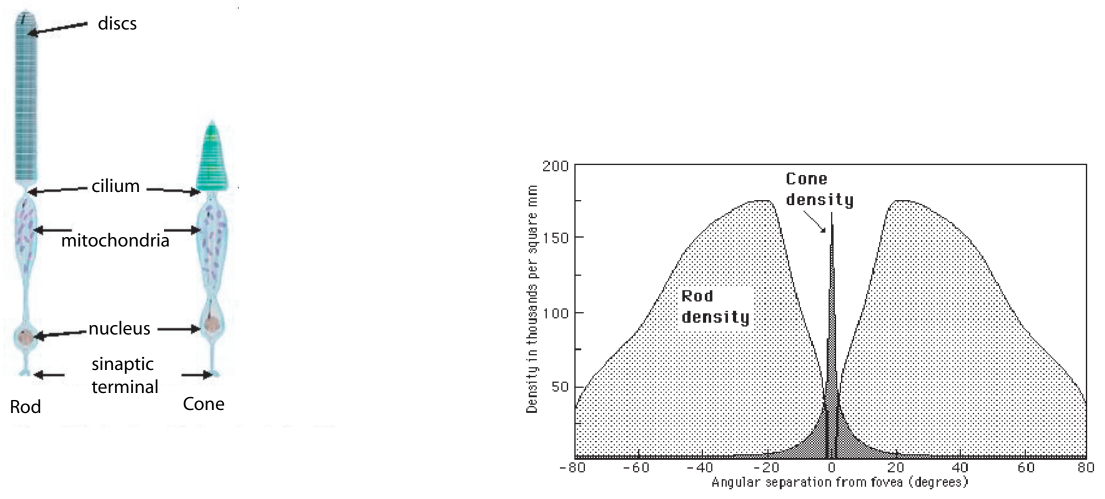


Figure 4.3: Rods and cones: *left* structure, *right* eye location distribution

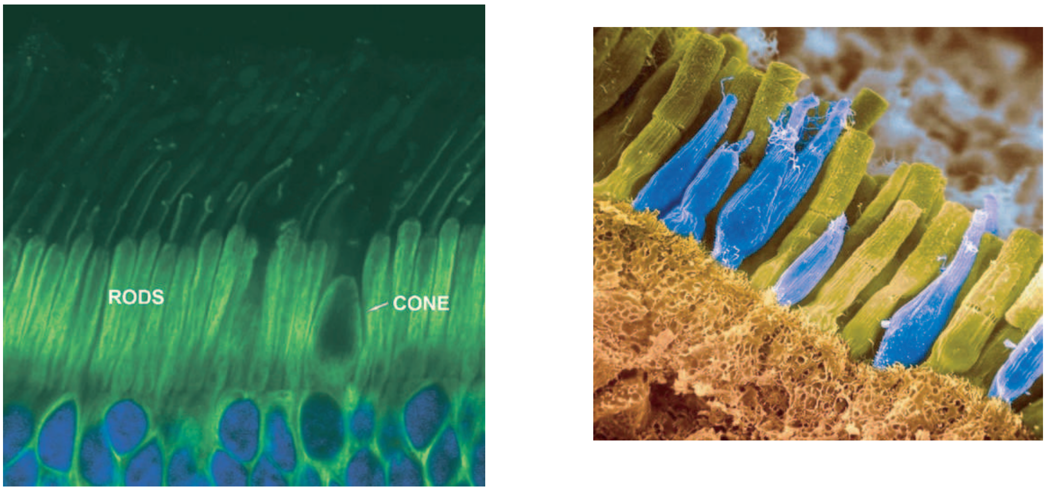


Figure 4.4: Magnified images of the photoreceptors.

pigmentation stabilizes during the adolescence, at older ages, the iris can change lose some of its pigmentation due to demelanization. Most eye-color changes have been observed in the Caucasian population with hazel eyes, although no studies have been performed over a population wide enough to draw general statements. In the cases of albinism, there is no pigment in the iris, so the eye color would be pink, according to the blood vessels of the eye (Figure 4.5).

The iris contains pigmented cells and muscle and is composed of four layers:

- The anterior border layer: a dense packing of pigmented or nonpigmented cells with a star shape.
- The stroma: a loose fibrocollagenous support issue associated with spindle- shaped fibroblasts (stromal cells), blood vessels, nerves and macrophages (clump cells of Koganei) containing phagocytosed melanin pigment; at the pupil margin is the circumferentially arranged smooth muscle of the sphincter muscle of the pupil.
- The dilator muscle layer: the fibers of the dilator muscle are derived from, and remain in continuity with, the cuboidal pigmented cell bodies which make up the anterior layer of iris pigment epithelium.
- The posterior epithelium: it is composed of two layers of cells which are densely pigmented with melanin to absorb light and reduce optic distortions.

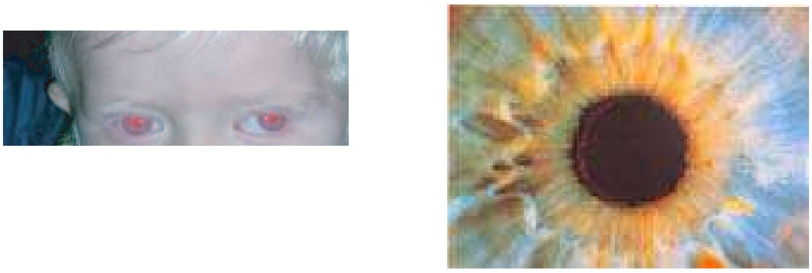


Figure 4.5: Special iris: example of ocular albinism (*left*) and iris demelanization (*right*).

4.4. Iridology

Such a characteristic human component has motivated different studies from ancient times. Eyes are known to be the most expressive part of the body, and there is people who claim to be able to prescribe other individual's mood based on their eyes. Interpretation of these organs has led to studies such as iridology, also known as iridodiagnosis. This is an alternative medicine technique which is believed to be born in Ancient Egypt, when eyes were considered as part of one's soul. Hieroglyphics tell stories of how examination of the patient's health was performed through the study of patterns and colors of his/her eye.

The first description of iridological principles are found in Philippy Meyerus' work of 1665, although true eye diagnosis wouldn't become popular until the 19th-century. Eyes are supposed to reflect past medical problems, illnesses and predict later consequences of developing health problems. To see this, iridologists match their observations of the eye to iris charts, which divide the iris into zones corresponding to specific parts of the human body. The details in the iris reflect changes in the tissues corresponding to body organs. Typical charts divide the iris into approximately 80-90 zones, as shown in Figure 4.6. Using magnifying glasses and cameras, practitioners distinguish between healthy organs and those inflamed or distressed.

Iridology does not belong to the conventional medicine, and iridologists are rarely physicians. The main criticism that is made to iridology is the fact that the iris does not undergo substantial changes in an individual's life, which is why it performs so good as a biometric trait. Therefore, critics support that there is no correlation between illness in the body and observable changes in the iris. However, iridologists defend themselves by pointing out the parallelism between the density in the iris fibers and the strength that human has toward illnesses. This means that it is possible a diagnosis of how an individual will react to a certain disease.

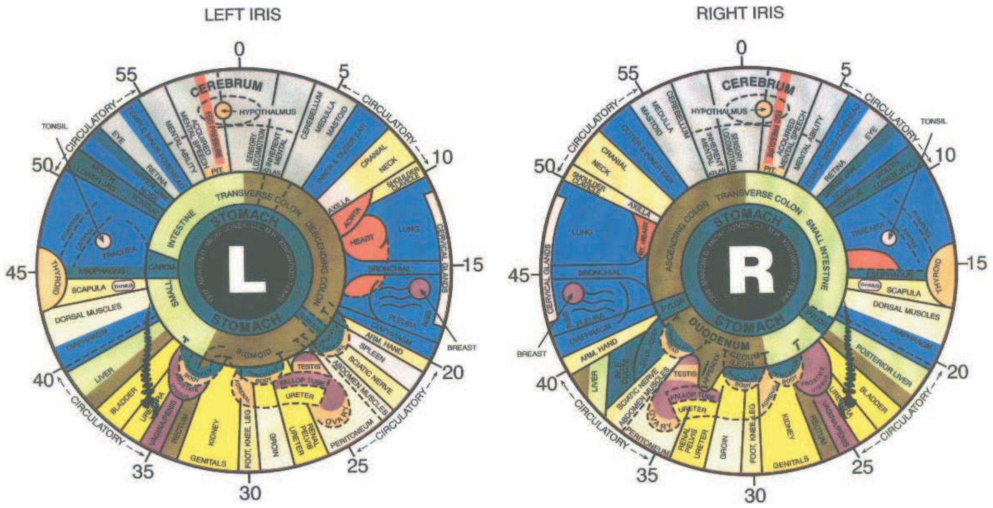


Figure 4.6: Iridology chart key

4.5. Iris acquisition

4.5.1. Introduction

The main problem of iris-based recognition is that the camera needs to be very close to the subject, no more than 40 cm from the sensor, which normally creates a sense of discomfort in the user. For a correct pattern extraction, the image needs to be centered and focused. However, the use of any support device, such as peepholes or face supports would only increase the sense of rejection of the system from the user which means that the system must be flexible and adaptable. To avoid any other disturbances for the user, the illumination needs to be carefully controlled, although sufficient to capture a high quality image. Altogether, the acquisition of an iris image represents a tough challenge, whether it uses manual or automatic processes.

New techniques are being developed toward a more user-friendly iris acquisition. Although some of these techniques are able to capture images from 3 meters away, they represent new challenges, this time in the social aspect. Systems which are able to capture biometric features without the individual's cooperation, or maybe even without his knowledge, are often seen as a threat for the person's privacy.

4.5.2. Traditional acquisition systems

The iris-scan process begins with a photograph. A specialized camera uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes only one to two seconds and provides the details of the iris that are mapped, recorded and stored for future matching/verification.

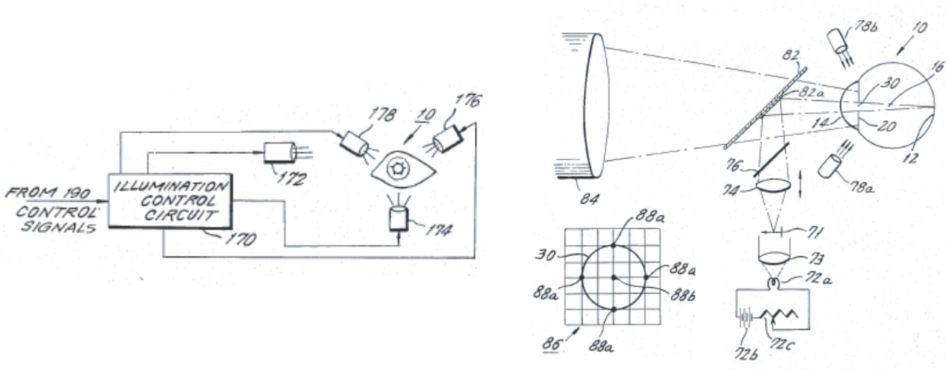
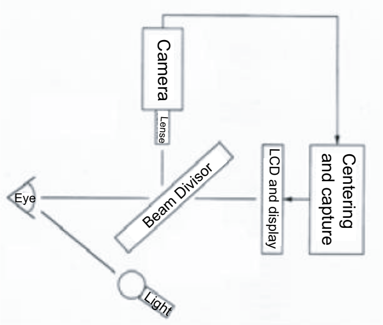


Figure 4.7: Flom and Safir's patented system. Source: [1]

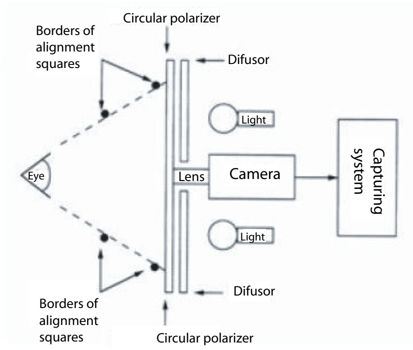
Although relatively new, iris recognition counts with several different acquisition systems. The first one, shown in Figure 4.7 was developed by Leonard Flom and Aran Safir [1], who were awarded with the first patent of this technique in 1987. This primitive system is based on four illumination points, three of them creating a 120 degree angle around the eye, and the fourth one in front of it. The iris pattern is captured by a lens from the reflected image produced by the eye.

Breakthrough work to create an efficient iris-recognition was pioneered by John G. Daugman [23]. Daugman's system illuminates the eye from an underneath point in order to achieve a diagonal incidence, and captures the reflected image with a specialized camera. The eye has to be within 45 cm of the device. This system, which is depicted in Figure 4.8 (*left*) results in an image between 100 and 2500 pixels of iris diameter with a 330mm camera diameter. This system was successfully utilized to debut commercialization of the technology.

The second most important modern system was deployed by Richard Wildes [24], also shown in Figure 4.8 (*right*). He uses two illumination points, one on top and one on the bottom of the



(*Daugman's system*)



(*Wildes et al's system*)

Figure 4.8: Acquisition systems

camera, and the image is directly captured by the camera with the eye 20cm away from the eye. The obtained image has an iris diameter of 256 pixels for 80mm of diameter of the objective.

Both these last systems capture a short video and choose the best frame among the sequence of images, but user cooperation plays a vital role in this technique to acquire a focused and centered image.

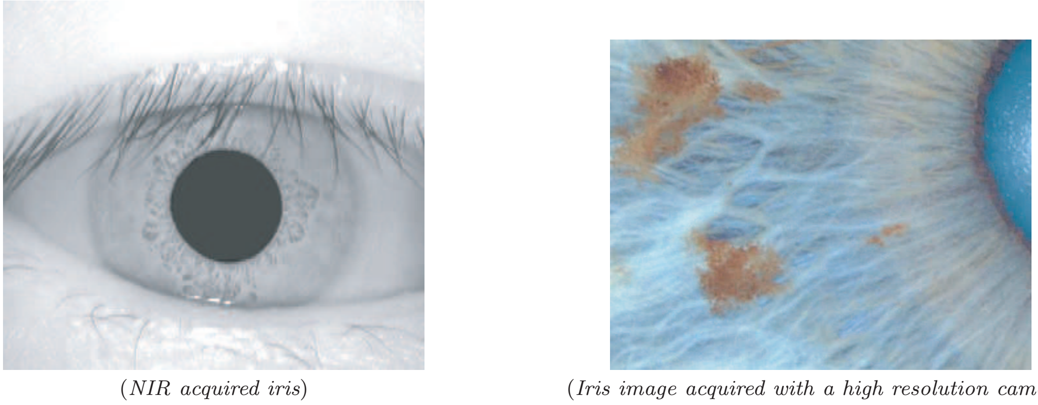
4.5.3. Iris recognition cameras

Although initially a standard photographic camera was used, one of the main problems in iris recognition is the acquisition of a high quality iris image while remaining non-invasive to the user. Currently, three main types of cameras [26] are adopted by commercial systems to acquire iris images. A comparison between them can be found in Table 4.1:

NIR iris camera. These cameras are most commonly used in current commercial systems due to the rich detailed images that they provide, even for dark color irises. It uses Iridian technology (i.e. the Daugman system) [27] with an illumination in the 700-900nm band. A typical NIR camera can capture iris patterns up to 60cm away, although the user's cooperation is still required. Images are captured in a black and white scale, with 256 grey levels. An example of a captured iris with this type of camera is shown in Figure 4.11. Some iris cameras, such as OKI IROSPASS-WG or Panasonic BM-ET 500, are able to capture both eyes simultaneously and perform identification based on both of the extracted features. The accuracy of these cameras is higher although the false rejection rate also increases. Enrollment and identification processes are also usually more complex on exchange of this extra security.

High-resolution color iris camera.Although color us a very distinctive feature in human eyes, its acquisition becomes quite complex when dealing with recognition systems. Dark pigments absorb the light and reflection is not good. Even for light colored irides, RGB cameras would have trouble capturing a complete image. Some studies are testing high-resolution color iris images to analyze iris patterns. For example, Miles Research Professional Iris Research Imaging System uses an iris camera based on an RGB video camera with resolutions as high as 6.144 x 4.096 as the one shown in Figure 4.11. However RGB cameras can only acquired detailed iris patterns in a distance as close as 5 cm. Therefore, the biggest challenge of this technology is the distance, which involves a much more intrusive acquisition process. Users discomfort limits the number of applications where iris recognition would deploy.

Telescope-type iris cameras.The biggest drawback of iris recognition is the need for the user's cooperation. This process can be bothering and thus, applications where it can be used are limited to close distance interactions.



(*NIR acquired iris*)

(*Iris image acquired with a high resolution camera*)

Figure 4.11: Examples of images acquired with NIR and High definition cameras

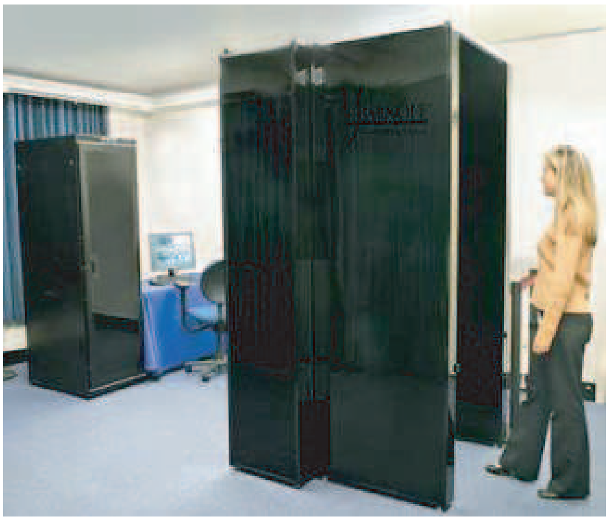


Figure 4.13: Iris on the move acquisition system.

However, Matey Group from Sarnoff Corporation has recently developed a new kind of iris acquisition camera, called IOM (Iris On Move) [28], shown in Figure 4.13. It is mounted on arcs as the ones found used for metal detection in the airports and allow iris detection when people are going through. It can acquire images up to 3m, and perform identification of 20 people per minute, which makes it useful for surveillance purposes. This iris camera uses a telescope-like lens and a strong NIR illuminator. The constructed lab prototype could result in eye damage if a user accidentally has a very close look to the illuminator. However, with more improvements to come, the system has a very strong de-blur performance using a 2048 bits code, which allow to distinguish between face and iris. This system may also include an identification based on a combination of eye-face features.

Characteristic	NIR camera	High-resolution camera	Telescope-type camera
Maximum operational distance	60cm	5cm	3m
Type of illuminator	NIR (700 900nm)	Visual light	NIR (700 900nm)
Typical resolution	640 x 480	6,144 x 4,096	Unknown
Commercial availability	Yes	Yes	No (lab prototype)
Applications	Iris identification	Iris pattern analysis	Iris surveillance
Challenges	Non-cooperative users	Intrusive capture. Short operational distance	Eye safety

Table 4.1: Comparative between iris acquisition cameras.

4.5.4. Illumination issues

It is important to remember that the iris size controls the amount of light that penetrates the pupil. Under poorly illuminated conditions, the pupil will expand in order to capture as much light as possible. This will result in a smaller iris pattern visible. However, under very bright conditions, the pupil will close to avoid damages in the retina, leaving a larger amount of iris visible. This variability, shown in Figure 4.14, needs to be taken into account since it may create false mismatches during comparison. Ideally, iris capture should always be performed under the same conditions.

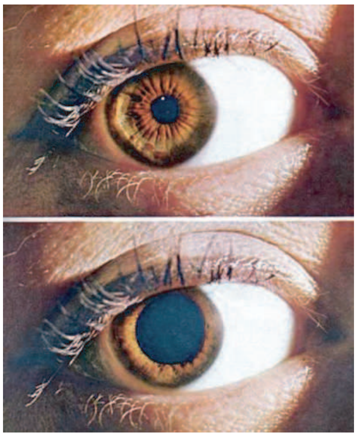


Figure 4.14: Contracted and dilated pupil.

During the acquisition of the iris, illumination needs to be enough to capture a good quality image but not so bright as to bother the user. The illumination during the acquisition of these images is typically provided by a near infrared light, whose energy is insufficient to cause any photochemical damage. By using a LED illuminator it is possible to minimize potential thermal damages as well, although it is important to design the system carefully if more than one device is going to be used. *Daugman's system* illuminates the scene with a single LED that is able to avoid eyeglasses reflection but not the redeye effect produced by reflection of the light in the cornea. *Wilde's system* is more sophisticated and it makes use of polarized filter and blurred light to avoid this reflection and achieve a detail-rich iris image. Nowadays, commercial systems use non-visible light to illuminate the iris, making the acquisition process less uncomfortable for the user.

4.5.5. Iris positioning issues

Iris-based recognition systems require user's cooperation. Despite capturing a sequence of images, not always there is one suitable enough for recognition. Focus and centered are some of the issues that systems need to deal with. Each patented system takes a different approach to overcome these difficulties. *Daugman's system* is based on a liquid crystal screen where the user can see his/her eye and adjust it to the correct position. The best image will be chosen among the video sequence according to certain contrast criteria (Figure 4.15). On the other hand, *Wilde's* *system* chooses optimality based on squares relative superposition. Iris is segmented in squares. When squares match, the iris is correctly adjusted and the image is then selected.

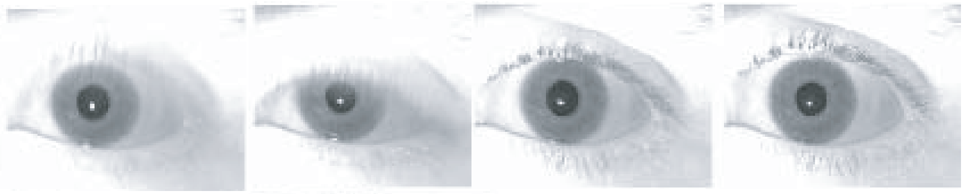


Figure 4.15: Succession of Iris images from a video sequence

The need for human supervision implies one more drawback for this technology. Therefore, today's efforts are focused on what it is called "iris on the move", as presented in Sec. 4.5.3. This new technique proposes an automatic iris capture from a face video sequence acquired as people walk through a dedicated portal. The aim of this technology is to make face and iris recognition practical in less-controlled conditions, by acquiring images in a more flexible manner and/or being able to use images of more widely varying quality. This is a direction that is currently attracting a number of research efforts, e.g. [29, 30, 31]

4.5.6. Commercial iris acquisition systems

Although iris recognition systems are still under development, several *security iris-based techniques* have been already implemented in today's society. Biometrics are gaining social acceptance by proving their efficiency in different fields. The ease of use and increase security over traditional security measures help biometrics' development and popularity.

From the three general applications of biometric systems, the one where iris recognition is more relevant is in security. In different parts of the world, border control has been automated and iris is being used as the identification feature. For example, the United Arab Emirates has been operating an expellee tracking system. All air and sea ports of entry in the country are equipped with these systems. The efficiency of this technique is supported by the 330.000 persons that have been apprehended re-entering the Emirates with fraudulent travel documents. Similar systems have been introduced in Pakistan for repatriation control aid and in different airports, were identification speeds up not only the security process but also boarding procedures. For example, at Schiphol Airport, in the Netherlands, iris recognition has permitted passport-free immigration since 2001. In the UK, Heathrow airport has also implemented an iris recognition program which is expected to get rid of passport controls in the next few years. Canada and USA have joined themselves to the list of countries experimenting with this technology with pre-approved, low-risk travelers.

Although its main impact is in security systems, the trend of biometrics leads toward more commercial applications. The use of portable iris systems integrated in devices such as cell phones, laptops or PDAs, open the possibilities of this technology to the general public. Any device with a good enough camera can be used as the security test for payment applications, account registration and others. In addition, the mentioned Iris On The Move acquisition is expected to expand the iris biometrics to a new range of applications in everyday life.

4.6. Iris segmentation methods

4.6.1. Introduction

Iris analysis begins with an automatic way for establishing whether an iris is visible in an image, and then locating its inner and outer boundaries (pupil and limbus). Generally, a pre-location process takes place, in which the eye is extracted from the rest of the image. This step distinguishes the zones of interest to speed up and increase the accuracy of the more sophisticated processes to come. Once this mission is accomplished, the detail of the iris is obtained. The main difficulty of this task comes from the fact that the shape of the object that needs to be segmented is not necessarily regular and the borders are not always well defined. There is a wide variety of segmentation methods. Initially, they focused on modeling both iris and pupil as two concentric circles. However, more recent techniques bet on irregular models for this contours.

The success of this step is crucial for the good performance of the rest of the system. A corrupted segmented iris pattern would lead into recognition errors. One of the key aspects that condition the success of the segmentation step is the image quality. Three main characteristics are responsible for this: *i*) sensibility to a high range of contrast between edges, *ii*) robustness between edge irregularities and *iii*) capacity to consider variable opening and closing processes.

4.6.2. Integro-differential operator

This is an outline fitting technique based on gradient optimization which was developed by Daugman [32] and it is by far the most referenced in the literature of iris recognition. It was initially proposed in 1992 and it was the first implemented effective system.

Daugman's method is based on the assumption that both the iris and the pupil can be modeled as circles. He developed an integro-differential operator to find circular pupil and limbus boundaries. The simplest interpretation of this process is a circular edge detector applied on a Gaussian filtered smoothed image that searches the parameters of a circular boundary along which the integral derivative is maximal. If the raw input image is defined as $I(x, y)$ and the objective circular contours from both the inner and outer iris borders are defined by its center (xc, yc) and its radius r, the equation that needs to be maximized relates to the luminance intensity at the point (x, y) through:

$$\left| G_\sigma(r) * \frac{\delta}{\delta r} \cdot \oint_{r,x_c,y_c} \frac{I(x,y)}{2\pi r} \mathrm{d}s \right| \tag{4.1}$$

where $G_\sigma(r) = (\sqrt{2\pi} \cdot \sigma) e^{-|(r-r_0)^2/2\sigma^2|}$ is the gaussian radial function centered at r_0 and standard deviation σ which allows to smooth out irregularities on the borders of the circular coronas; the symbol $*$ implies convolution, ds shows circular differential segment and $2\pi r$ is used to normalize the integral.

The complete operator behaves as a circular edge detector, and it searches iteratively for a maximum contour integral derivative with increasing radius at successively finer scales of analysis. A number of improvements over this method have been developed. Among the most important ones it is necessary to highlight:

- *Histogram equalization.* The segmentation process generally improves when the contrast between different eye regions is enhanced.
- *Binarization.* Based on the same principle, setting a threshold in an image before applying the operator can increase the differentiation of regions in the image.

Besides improvements added to the algorithm, some works such as [33] have modified and optimized it for frontal iris individual images. Camus and Wildes search and optimize the three reference parameters of a circumference (center (x, y) and radius(r)) in a tridimensional space (N^3), through the formula:

$$C = \sum_{\theta=1}^{n} \left((n-1)||g_{\theta,r}|| - \sum_{\phi=\theta+1}^{n} ||g_{\theta,r} - g_{\phi,r}|| - \frac{I_{\theta,r}}{n} \right) \tag{4.2}$$

where n is the total number of directions and $I_{\theta,r}$ and $g_{\theta,r}$ correspond to the image intensity and its derivations respect to the radius in the polar coordinates system respectively.

Another variation of Daugman's system is presented by Sanchez-Avila et al. [34]. This method aims to maximize the means of the intensity differences of the five consecutive differences defined as follows:

$$D = \sum_{m} \left(\sum_{k=1}^{5} (I_{n,m} - I_{n-k,m}) \right) \tag{4.3}$$

where $I_{i,j} = I(x_0 + i\nabla_r cos(j\nabla_\Theta), y_0 + I\nabla_r sin(j\nabla_\Theta))$.

The parameters ∇_r y ∇_Θ are the radius and angle increments respectively; $I(x, y)$ is the image intensity. This method finds the three parameters of a circumference (center (x, y) and radius (r)), where the intensity difference between five successive circumferences is maximum.

One of the most recent techniques following the Daugman approach tries to solve the problem of segmentation for off-angle iris images. Dorairaj et al. [35] assumes the magnitude of the rotation is known and uses Daugman's objective function to perfect the estimation, achieving a frontal view of the rotated image.

4.6.3. Canny-based edge detector

In 1997, Wildes proposed a two-stage iris segmentation method which makes use of the Canny edge detector and the Hough transform [36]:

1. A gradient-based binary edge map is first constructed from the intensity image (see Figure 4.16). It can be obtained as:

   $$|\nabla G(x, y) * I(x, y)| \tag{4.4}$$

   where $\nabla \equiv (\partial/\partial x, \partial/\partial y)$ and $G(x, y) = 1/2\pi \cdot \sigma^2 \cdot e^{-\frac{(x-x_0)^2+(y-y_0)^2}{2\sigma^2}}$ is a bidimensional Gaussian function centered at (x_0, y_0) and the standard deviation σ that allows to smooth out edge irregularities.

   The edge image is then constructed through the gradient, which uses a Canny edge detector. A directional adjustment is added to the system by weighting the edge detection by the orientation range to improve the segmentation. The reason for this directional adjustment is that, for the outer limits of the iris for example, the vertical direction is the predominant, and therefore, edge detection should be applied in that direction (see Figure 4.16, fourth image).

2. The inner and outer boundaries are then detected via Hough transform. This is the most common method used for iris segmentation. It allows recognition of global patterns in the image, finding local patterns (ideally a point) in a transform parameter space. The basic operation of this technique is to find curves such as lines, circles, polynomials, etc. that can

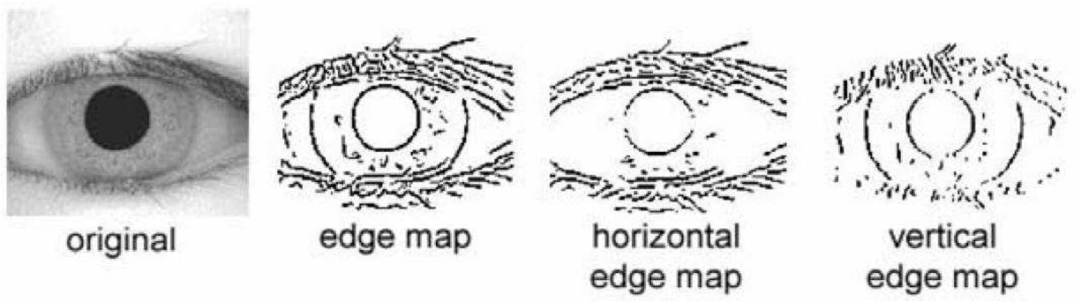


Figure 4.16: Transition of contour images

be located on a proper parameter space. It uses a parametric representation of geometric shapes. For example, a line could be represented by a module ϕ, perpendicular to the line that crosses the origin $(0,0)$, and an angle ρ, composed of the module and positive x's axis. A general representation of two of the most used shapes is as follows:

$$\textit{Line equation}: \; x\cos(\rho) + y\sin(\rho) = \phi \tag{4.5}$$

$$\textit{Circle equation}: x_c^2 + y_c^2 = r^2 \tag{4.6}$$

Its use is mainly focused on two-dimensions, for straight lines, centers of circles with a fixed radio, etc., although it can also be used for higher dimensions. This transform is particularly useful for noisy information. However, the image construction requires a thresholding value which limits the system's robustness.

In general, Wilde's method is convenient since it avoids singularities such as infinite slope lines. When representing ϕ and ρ on a Cartesian plane, a point would be defined as a sinusoidal function, whereas a line would be represented by a point with coordinates (ϕ(line),ρ(line)).Two points would involve two sinusoids out of phase by α degrees, depending on the coordinates of the points. The geometric interpretation of this fact is that the sin function represents the infinite lines that cross each point. When two points share the same line, their sinusoidal representations will cross in the point of the plane (ϕ, ρ) that represents the line. This gives a point. When $\rho = 180°$, the same line is repeated, and therefore, another point is obtained.

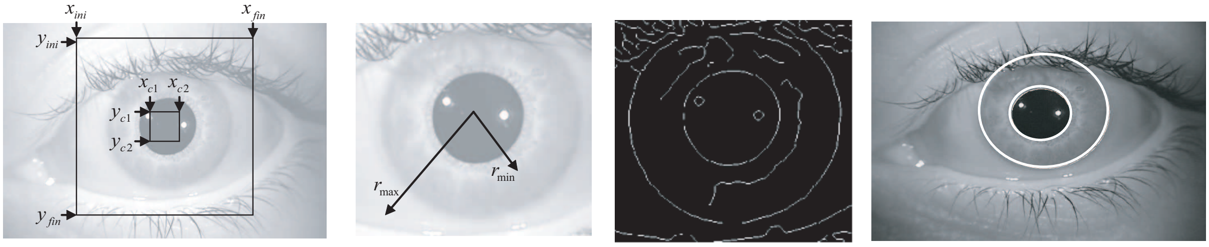


Figure 4.17: Steps of the Hough transform for circle detection.

This algorithm is mainly used for locating the circumferences that demarcate the iris region. In Figure 4.17 it is shown that the square $(x_{ini}, x_{fin}, y_{ini}, y_{fin})$ defines the search window for possible circumference edge points, and the square $(x_{c1}, x_{c2}, y_{c1}, y_{c2})$ defines the possible center points of those circumferences. The algorithm evaluates for each center, all the possible circumferences through the equation 4.6, assigning a certain scored based on how many edge pixels it includes. Based on the maximum score, the algorithm will finally chose the circumference which best adjust itself to the iris, defining then the parameters that describe the selected circumferences.

A parabolic Hough transform can also be used to detect eyelids. Both top and bottom eyelids can be defined through parabolic eyelids, represented as:

$$(-(x-h_j)\sin\theta_j + (y-k_j)\cos\theta_j)^2 = a_j((x-h_j)\cos\theta_j + (y-k_j)\sin\theta_j) \tag{4.7}$$

where a_j adjusts the curvature, (h_j, k_j) is the peak of the parabola and θ_j is the rotation angle with respect to the x-axis.

Different orientations will be used to detect eyelid and iris, as shown in Figure 4.16. Eyelids are horizontally aligned, and therefore their extraction will be best following the horizontal direction. Iris border will be localized using only the vertical direction, which will reduce the eyelid effect when applying the circular Hough transform. Thus not all edge pixels that define a circumference will be used for localization making the process efficient and less computationally costly, but still very accurate.

The main disadvantage of the Hough transform is the need of a threshold to declare an edge. An incorrect decision can lead to a contour free image, and the circles/arc will not be correctly defined due to a lack of edge points. Another issue that must be taken into account is the computational strength that the Hough transform requires. The brute force method that it uses makes it non suitable for real time applications.

One of the many studies that tries to optimize this technique is the one by Liu et al. [37], who tries to simplify the method by assuming that pupil and iris are concentric. Huang et al. [38] suggests that the transform computational cost can be reduced by conducting first a coarse search on a re-escaled smaller image, and apply the results to optimize the search over the original larger image. Sung et al. [39] improves this methods by introducing a histogram equalization technique followed by a high frequency filter. Another solution is proposed by Lili and Mei [40], who assume three well defined points in the image histogram, corresponding to the pupil, iris and sclera, to improve localization. Shi [41] applies an image binarization to localize the pupil and after a contour detection, he uses a Hough transform. Tian et al. [42] estimates the center of the pupil through the pixels with a grey level below a certain threshold before applying the Canny edge detection and the Hough transform. Zaim et al. [43] detects regions of interconnected points of uniform intensity. Xu et al. [44] aims for a lighter computation algorithm by dividing the image in a rectangular grid and estimating the average intensity in each cell; the pre-location of the pupil can be then chosen finding the cell with the smallest luminance, which should correspond with the almost completely black pupil. Based on the same principle of the pupil region having the pixels with the smallest grey levels, Sun et al. [45] estimates the pupil and then applies the Canny and Hough algorithms.

4.6.4. Other methodologies

The weaknesses that the previous methods present combined with the increasing interest on iris recognition have induced many different techniques for iris location and segmentation.

One of the alternatives is presented by Bonney at al. [46], with a series of *dilation and compression operations* on the image. Once the pupil is found, the standard deviation is computed in both the vertical and horizontal direction, in order to find the pupil and iris boundaries, which will be defined as ellipses.

El-Bakry proposed in [47] the use of neuronal webs for iris segmentation, but he never obtained experimental results. More recently He et al. [48] presented a work based on *Viola and Jones Cascade Classifiers* [49] for optimum pupil region detection.

Tuceryan [50] presented a method of *texture based segmentation*, which uses the moments of small windows of the image as characteristic features on which apply a clustering algorithm to segment the image. The second order of geometrical regular moments for each image pixel can be computed using:

$$M_{pq} = \sum_{\frac{-W}{2}}^{\frac{W}{2}} \left(\sum_{\frac{-W}{2}}^{\frac{W}{2}} (I(m,n) x_m^p y_n^q) \right) \tag{4.8}$$

where M_{pq} is the geometric regular moment of order pq, $I(m,n)$ is an intensity pixel from the image, x, y the window coordinates and W its width.

After the experiments, Tuceryan concluded that the ordinary moments were not discriminative enough and proposed the use of the hyperbolic function as a lineal transduction followed by an averaging of:

$$F_{pq}(i,j) = \frac{1}{L^2} \sum_{(a,b) \epsilon W_{ij}} W_{ij} \big(\tanh(\sigma(M_{pq}(a,b) - \bar{M})) \big) \tag{4.9}$$

where F_{pq} is the characteristic image of the moment M_{pq} whose mean is $\bar{M}$, and W_{ij} is a median window of size L x L centered at (i,j); σ controls the shape of the logistic function.

Li [51] uses an ellipse to fit the pupil boundary and then applies a rotation and scaling to transform the image off angle and turn it into a circumference. In 2005, Abhyankar et al. [52] showed that segmentation based on circular boundaries was worst when the iris was off angle. Works in [53, 51] also consider projective transformations, although some drawbacks such as outside edge blur limit its use. To solve this, they present a method based on biorthogonal wavelet net.

More recently, in [54], a new modeling technique is presented. Active contour models are used to find the elliptical iris shape on off-angle images. Among these new segmentation methods and techniques, is also important to mention the ones which use texture analysis [55] and nested cuts [56].

4.6.5. Segmentation problems: noise and eyelashes detection

Segmentation is greatly affected by noise and eyelashes. This is the main reason why researchers are making such a big effort to localize them and reduce their effect. Other problems that affect segmentation are non-centered irides, off-angle irides, rotated iris images, blurred iris images, obstruction due to glasses or eye contacts, iris images containing specular or illumination reflections, partially captured irides or images without an iris.

Kong and Zhang [57], implemented a method to detect eyelashes. He classified them as separable, which can be isolated from the iris region, or non-separable, which will be accumulated and superposed on the image. The separable eyelashes can be detected using 1D Gabor filters, since their convolution with the Gaussian smoothing function would have a small level value. The smallest resulting value corresponding to one of the eyelashes would establish the threshold. Multiple eyelashes would be detected using the intensity difference. If this difference in a small window is less than a threshold value, the center of the window would be considered as a point of an eyelash. This model also makes use of connective criteria: each point on an eyelash must be connected to another point of an eyelash or eyelid. Specular reflections on the eye image are detected through umbralization, since the intensity value in these regions will be higher than anywhere else in the image.

Huang et al. [58] uses phase consistency to obtain edge information and find noise boundaries and occlusion regions. Some recent works, such as [59], take similar approaches to improve the detection of eyelid and eyelashes occlusion and specular reflections.

The work in [60] presented by Bachoo and Tapamo take a different approach to the occlusion problem. A co-occurrence matrix technique based on the grey levels of an image (GLCM) is used to detect occlusion due to eyelashes. The GLCM is computed for 21 x 21 image windows through the 64 most significant grey levels. Based on the characteristics of this GLCM, and algorithm is applied to the windows divided in groups from 2 to 5 different types (skin, eyelashes, sclera, pupil and iris). The disadvantages of using this method are the election of the window size and how to deal with the windows which contain more than one type.

Libor et al. [61] use a system based on the Hough Linear transform to perform the eyelashes detection. Eyelids are detected by applying noise masks created through a thresholding of the grey level histogram.

4.6.6. Methodology comparison

Proenca et al. [62] carried out a comparison of the most popular segmentation methods, which is summarized in the Table 4.2. The first column identifies the evaluated method, the second the modifications performed over the original method and the third and forth columns show the obtained segmentation results over the UBIRISv1 database, which contains images acquired in two sessions, with high quality for first session and lower quality for the second. The fifth column shows the degradation of performance between the first and the second session of captured images, and the last column shows the execution time (in seconds) of the method.

Method	**Parameter**	**Session 1, %**	**Session 2, %**	**Degradation, %**	**Time, s**
Daugman	Original	95,22 ± 0,015	88,23 ± 0,032	6,99	2,73
Daugman	Ecualization histogram	95,79 ± 0,014	91,10 ± 0,028	4,96	3,01
Daugman	Binarization	96,54 ± 0,013	95,32 ± 0,021	1,22	2,92
Wildes	Original	98,68 ± 0,008	96,68 ± 0,017	2,00	1,95
Camus y Wildes	Original, 8 directions	96,78 ± 0,013	89,29 ± 0,030	7,49	3,12
Martin-Roche et al.	Original	77,18 ± 0,030	71,19 ± 0,045	5,99	2,91
Tuceryan	Total Cluster=5	90,28 ± 0,021	86,72 ± 0,033	3,56	4,81

Table 4.2: Methodology comparison between different de segmentación techniques. Experiments were carried out on UBIRISv1 database.

The segmentation results of the other methods mentioned in previous sections can be found in Table 4.3 as reported by their authors. In this chart are shown the most recent techniques which result in a higher performance. This success rate aims for a perfect ideal segmentation as technology evolves, to obtain a segmented image that can be used for reliable recognition.

First Author	**Year**	**Database**	**Segmentation results**
Camus	2002	640 images without glasses and 30 images with glasses	99.5 % 66.6 %, Total= 98 %
Sung	2004	3167 images	100 % iris segmentation, 94.54 % contour correct locations
Bonney	2004	108 CASIAv1.0 and 104 USNA images.	99.1 % correct pupil extraction 66.5 % correctly extracted contours
X. Liu	2005	4249 images	97.08 % recognition range
Lili	2005	2400 images of CASIA dataset.	99.75 % extracted correctly
Proenca	2006	UBIRIS dataset: 1214 images of good quality, 663 noisy.	98.02 % of good quality 97.88 % of noise
Abhyankar	2006	1300 images of CASIAv1 y WVU	99.76 % correct
Z. He	2006	1200 CASIA	99.6 %
X. He	2006	1200 CASIA	99.7 %

Table 4.3: Comparison of the different segmentation methods.

4.7. Size normalization

For a reliable recognition, it is important to remember that acquired irides have variable sizes mainly due to the dilation and size of the pupil before different illumination levels (see Sec 4.5.4). The distance from the camera, the camera rotation or the head rotation during acquisition are other sources for iris size variation. Although the latter factors have been mainly alleviated by imposing constrained and collaborative acquisition procedures, new scenarios such as the Iris On The Move will need to cope with them. This fact makes a normalization step necessary, in order to create an invariant representation for all of the images, independently of the conditions under which they have been acquired. Another reason for the need of normalization is the fact that the pupil region is not always perfectly concentric in the iris region [63].

Different normalization algorithms have been proposed to deal with these problems and other related. The main ones are presented below.

4.7.1. Rubber sheet model

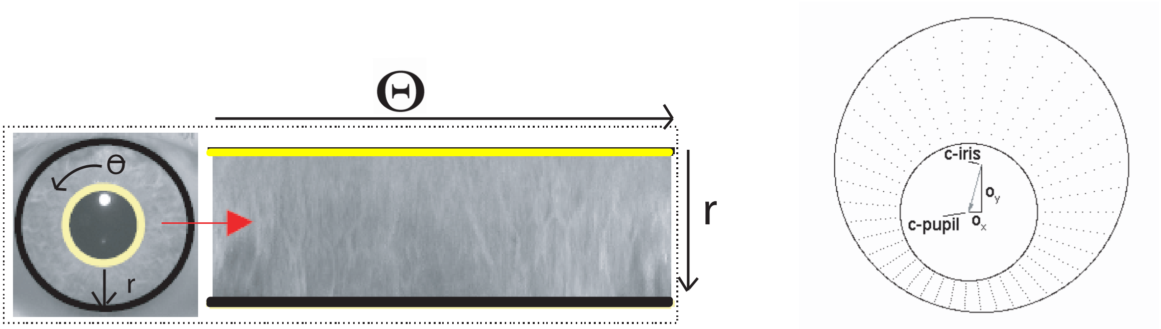


Figure 4.18: Examples of Daugman's method: normalization (*left*) and sampling (*right*)

Included in his iris-recognition system, Daugman developed a model which assigned each point in the previously detected anular iris region to a pair of polar coordinates (r, θ), where r is delimited between $[0, 1]$ and θ is the angle variation between $[0, 2\pi]$. The ring-shaped region of the iris is then converted to a rectangle of fixed dimensions as shown in Figure 4.18, achieving in this way invariance to pupil dilation and acquisition distance. The redistribution from Cartesian coordinates (x, y) to the non-concentric iris region representation in polar coordinates is shown in Figure 4.18 and can be modeled as follows:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta) \tag{4.10}$$

$$x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta)y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta) \tag{4.11}$$

where $I(x, y)$ is the iris image region, (x, y) are the original cartesian coordinates, (r, θ) are the normalized polar corresponding coordinates, and x_p, y_p and x_l, y_l are the coordinates of the inner and outer iris boundaries along the θ direction. This model takes into account the pupil dilation and the variable size of the images, in order to produce a normalized representation of constant dimensions.

A general interpretation of this method is that the iris is modeled as a rubber sheet, which accounts for the pupil dilation, the distance of image acquisition and the non-concentric pupil displacements as shown in Figure 4.18 (*right*). However, it can not account for rotation incoherencies, which will be included in the algorithm during the matching process through a θ rotation until alignment between the two iris under comparison is achieved.

4.7.2. Image registration

Wildes' system [64] uses an image registration technique which geometrically deforms the acquired image, $I(x,y)$, to align it with the selected database image, $I_a(x,y)$ [36]. It works directly on the ring-shaped iris image. The mapping function $(u(x,y),v(x,y))$ used to transform the original coordinates to the values of the new image, is used based on a nearest neighbor criteria of the corresponding reference points of the image. Therefore, the mapping function must minimize the function:

$$\int_x \int_y (I_d(x,y) - I_a(x-u, y-v))^2 \, dx \, dy \tag{4.12}$$

It must also perform a coordinate transformation from (x,y) to (x',y') such as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - sR(\phi)\begin{pmatrix} x \\ y \end{pmatrix} \tag{4.13}$$

with s as a scaling factor and $R(\phi)$ a matrix which represents the rotation by ϕ. The deformation parameters s and ϕ are computed through and minimization iterative process [36].

4.7.3. Virtual circles

Another possible solution for the normalization process is the one proposed by Boles [65]. In his system, iris images are first scaled to have a constant diameter so when two images are compared, one can be considered as the reference image. The difference with other techniques is that normalization will not be performed until two iris regions match, instead of performing normalization and storing the results for a later comparison.

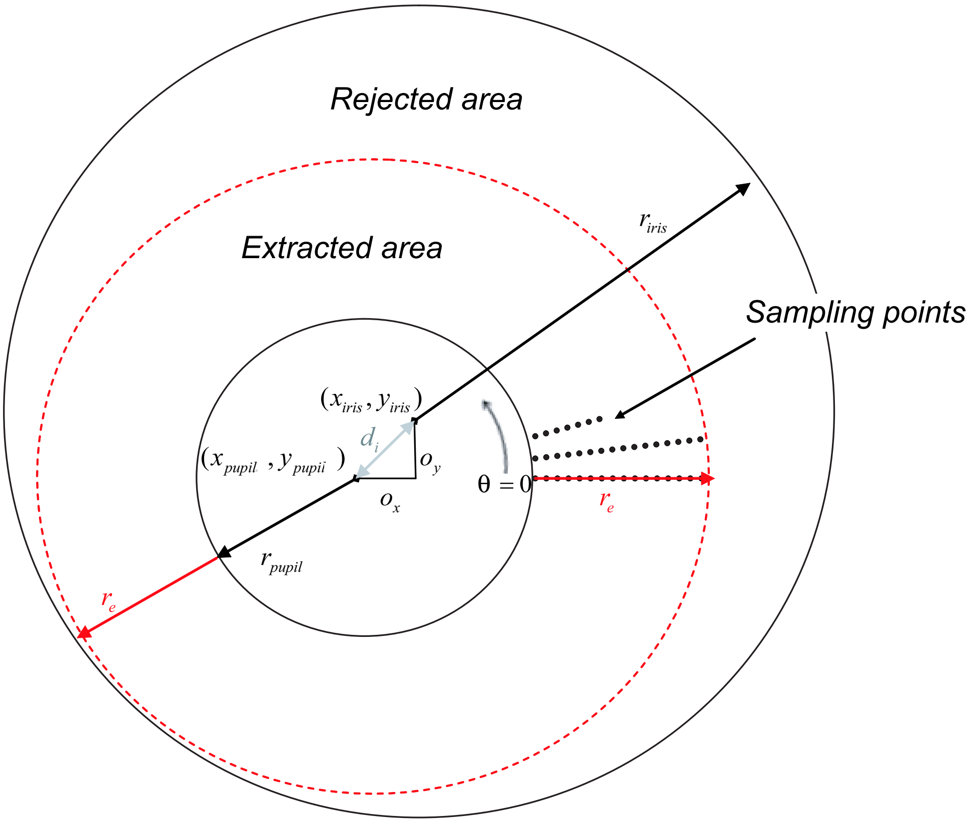


Figure 4.19: Description of the virtual circles normalization technique .

Once both irides have the same dimensions, the characteristics of the iris region are extracted in two steps. First the intensity values along the virtual concentric circumferences, which have their origin in the pupil, are stored. A normalization technique is then applied so that the number of extracted points in both irides is the same (Figure 4.19) . This technique is basically the same as the one used by Daugman except for the fact that expansion is related to time and iris region comparison instead of expanding the iris to a constant dimension. However, Boles does not mention how to achieve rotation invariance.

One variant from this technique is the one exposed in [66], known as *Iris Signature* (IS). This method is based on extraction by circumference. It also considers the centroid of the pupil as a reference point, so it extracts the grey levels of the contour of a virtual circle of the pupil, which is called iris signature. In Figure 4.20 one can see the iris signature corresponding to the virtual circle with radius r = r(pupila) + 20 píxeles.

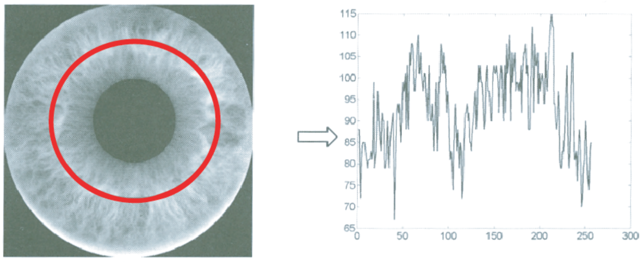


Figure 4.20: *Iris signature* from a circunference

An evolution of this technique [66] extracts a circular corona and considers the IS as a one dimensional signal, shown in Figure 4.21. This signal is computed as follows: the value of the IS at each point will be the mean of the grey values of all virtual iris circumferences, centered on the centroid with radius r, such that $r_i \leq r \leq r_e$ (mean of the circumferences inside the circular corona with inner radius r_i and outer radius r_e).

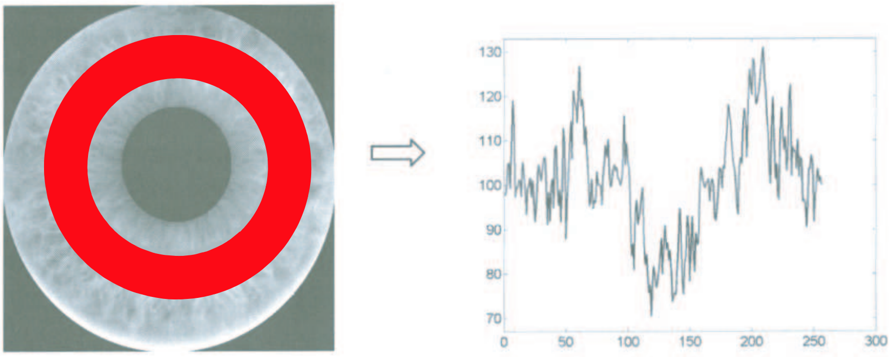


Figure 4.21: *Iris signature* from a circular corona

4.7.4. Angle normalization

The feature extraction process can sometimes be optimized by making a data transformation so that they superior and inferior regions of the iris are suppressed. This is because potential eyelids and eyelashes tend to be situated in these regions. To do so, a radius and angle sampling procedure is performed through the following equation system:

$$J(x,y) = IE(x_0 + r\cos\theta, y_0 + r\sin\theta)$$
$$r = r_i + (x-1)\nabla_r \qquad ,\forall x \epsilon N : x \leq \frac{r_e - r_i}{\nabla_r} \tag{4.14}$$

$$\theta = \begin{cases} \frac{-\pi}{4} + (y-1)\nabla_\theta & ,if \qquad y \leq \frac{\pi}{2\nabla_\theta} \\ \frac{\pi}{4} + (y-1)\nabla_\theta & ,if \qquad y > \frac{\pi}{2\nabla_\theta} \end{cases} \qquad \forall y \epsilon N : y \leq \frac{\pi}{\nabla_\theta} \tag{4.15}$$

where $J(x,y)$ is the new image, $IE(a,b)$ is the iris image with the extracted sclera and the pupils, r_i and r_e are the inner and outer radius, (x_0, y_0) is the pupil center, and ∇_r and ∇_θ are the magnitude and angle sampling intervals respectively.

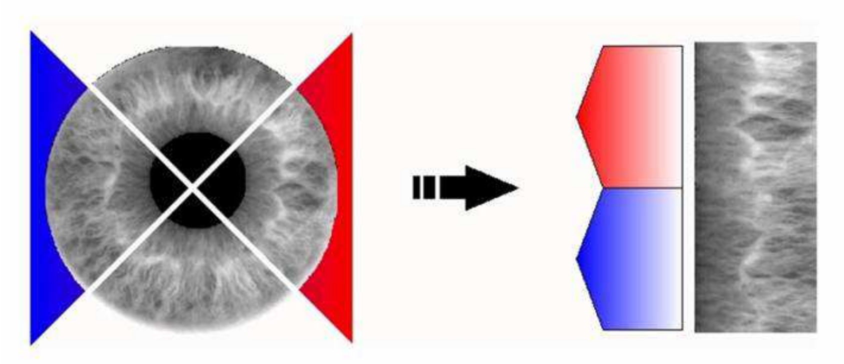


Figure 4.22: Normalization example for 45°.

Since sampling is performed between the outer and the inner iris edges, the same number of points will be used throughout the images, simplifying with this the subsequent feature extraction procedure. Figure 4.22 show a visual representation of this transform, were it can be seen that through sampling, the side cones of the iris are transformed into a square image. The columns of this image will correspond to fractions of the radius while the rows can be identified as angle increments. Together they make up a rectangular matrix which will always have a constant size (since the number of sampling points will be constant).

4.7.5. Contrast Enhancement and Noise Reduction

Once the iris region has been transformed into a constant size rectangle, a step of contrast enhancement can be performed to improve the extraction of features. One possible method to do so is as follows [67]. The background illumination is estimated and then removed from the original image through the following steps (see Figure 4.23):

1. The brightness variations along the image are estimated and the average luminance is computed for 16 x 16 blocks, interpolating it then to the whole image.
2. The estimated brightness variation is subtracted to the original image and histogram equalization is then performer on regions of size 32 x 32.

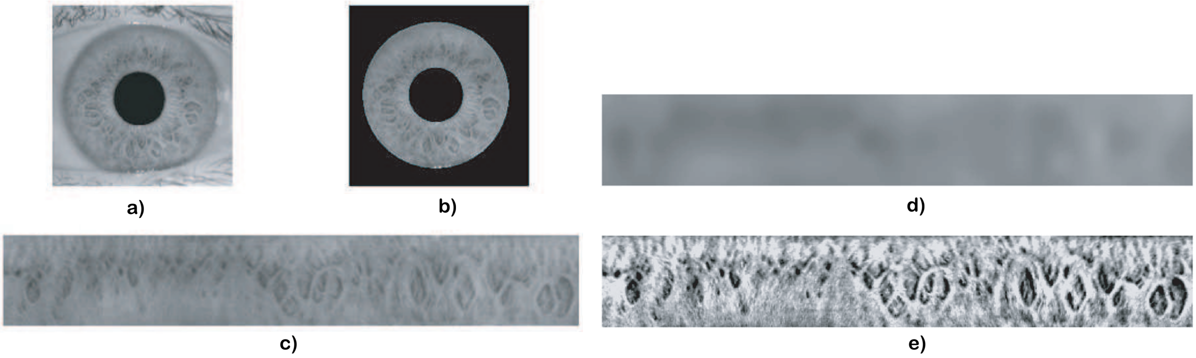


Figure 4.23: a) Original image, b) Located iris, c) Normalized image, d) Estimated background illumination and e) Resulting image after contrast enhancement.

4.8. Feature Extraction Methods

The uniqueness and discriminative degree of the characteristics extracted during this step will determine the reliability of the recognition. Therefore, redundant information must be discarded. A quantifiable set of features will be assigned to each iris pattern obtained in this step, which will allow the computation of a similarity measure between two iris patterns. To make a reliable decision about the identity of an iris pattern, the similarity value must be within a pre-defined range when the patterns are generated by the same eye, known as interclass comparisons, and within a different range when patterns created by different eyes are compared, known as interclass comparisons.

Different techniques lead the feature extraction process [9], which can be classified into: *i*) the Daugman approach, making use of Gabor filters and obtaining a binary representation of the iris called IrisCode; *ii*) alternative approaches making use of something other than a Gabor filter to obtain a binary representation; and *iii*) other approaches making use of different types of filters to represent the iris with a real-valued feature vector. The following is a description of the most common techniques used within these groups.

4.8.1. Binary IrisCode using Gabor filters

For his system [63], Daugman developed a method based on Gabor filters to perform the extraction and codification of features. A Gabor filter is created from the modulation of a sinusoidal/cosenoidal wave. It can provide an optimal location in both space and frequency. A sinusoidal wave is completely localized in frequency but not in space. The modulation with a Gaussian provides the spatial location, in exchange of some of the frequency location precision. The signal decomposition can be achieved through a Gabor filter quadrature, with a real part given by a Gaussian modulated cosine and an imaginary part given by a Gaussian modulated sine. The real and imaginary filters are also known as the odd symmetric and even symmetric respectively. The filter's center frequency is given by the frequency of the sinusoidal/cosenoidal wave, and its bandwidth by the Gaussian's width.

Daugman uses a 2D version of the Gabor filters to codify the iris patterns. In the image (x, y) domain, 2D Gabor filters are defined as:

$$G_{\theta,f}(x,y) = \exp\left\{\frac{-1}{2}\left[\frac{x'^2}{\sigma_{x'}^2} + \frac{y'^2}{\sigma_{y'}^2}\right]\right\} \cdot \exp\left\{2\pi f j x'\right\}, \tag{4.16}$$
$$x' = x\sin\theta + y\cos\theta$$
$$y' = x\sin\theta - y\cos\theta$$

where (x, y) specifies the position in the image, $f = \frac{1}{T}$ is the sinusoidal wave frequency in the θ direction with respect to the x axis, and $\sigma_{x'}$ and $\sigma_{y'}$ specify the width and length of the gaussian enfolding function along the x' and y' axis respectively. A representation of the impulse responses of a sinusoidal and a cosenoidal filter for the same angle in the spatial domain can be seen in Figure 4.24, where $\sigma_x = 8$, $\sigma_y = 4$ and $T = 11$.

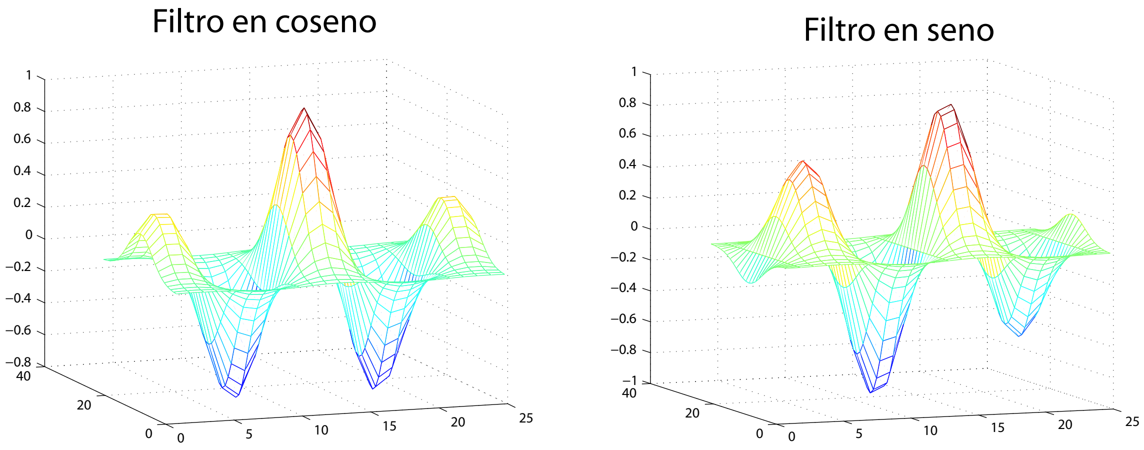


Figure 4.24: Gabor filters of size 25 × 25.

Once the Gabor filters are applied to the normalized iris image (following the method of Sec. 4.7.1), the output is demodulated to compress the data. One way to achieve this compression is to quantify the in-phase information in 4 levels in the complex plane, one for each possible quadrant. Oppenheim and Lim [68] have proven that in-phase data gives more significant information of an image than information of illumination, given by the amplitude. Therefore, only the information concerning the phase will be stored, discarding any other data including illumination. To represent these four levels, 2 bits are required. Therefore, each pixel of the normalized iris model will correspond to two bits in the iris pattern. The output generated pattern by using the Daugman method, known as *iriscode*, is 2048 bits long (256 bytes), and allows an efficient and fast comparison between two irides in the binary domain.

4.8.2. Binarization without using Gabor filters

An alternative to the previous method aims to create a *binary iriscode* similar to Daugman's using other filters rather than Gabor filters. The use of many different filters has been studied. Those filters which result in good results are explained next.

Log-Gabor filters

The main disadvantage of Gabor filters is that even a symmetric design will have a continuous component, which will require a bandwidth higher than an octave [69]. An easy way to remove this constant component is to use a Gabor filter in the logarithmic scale, known as Log-Gabor filter. The answer of this kind of filter is given by:

$$G(f) = \exp\left(\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right) \tag{4.17}$$

where f_0 represents the central frequency and y σ the filter's bandwidth. The details of Log-Gabor filters can be found in [69].

Wavelets

Wavelets have the ability to decompose iris data in different resolutions. Since the frequency of the data is localized, it allows an easy comparison of the characteristics in the same position and resolution. To do so, a series of wavelet filters, also known as wavelet bank, are applied to the 2D iris region, one for each resolution and scaled version. The codification of the results from this operation gives a compact representation of the iris patterns.

Wavelets have been extensively used for codification. There are different types of wavelets: Haar, Daubechies, Biorthogonal, Coiflet, Symlet and Gabor. In the following, the most important ones will be explained. A deeper analysis of these filters can be found in [70, 71, 72, 73].

- **Zero-crossings of the 1D wavelet transform**

  Boles and Boashash use 1D wavelets to codify the iris pattern in [65]. The master wavelet is defined as the second derivative of a smoothing function:

  $$\psi(x) = \frac{d^2\theta(x)}{dx^2} \tag{4.18}$$

  The zero crossings of the dyadic scales of these filters are the most significant points of the iris region and therefore, they are used to codify the characteristics. The wavelet transform of a signal $f(x)$ in a scale s and position x is given by:

  $$W_s \cdot f(x) = f * \Big(s^2 \frac{d^2\theta(x)}{dx^2}\Big)(x) = s^2 \frac{d^2}{dx^2}(f * \theta_s)(x) \tag{4.19}$$

  where

  $$\theta_s = (1/s)\theta\big(\frac{x}{s}\big) \tag{4.20}$$

  $W_s \cdot f(x)$ is proportional to the second derivative of $f(x)$ smoothed out by $\theta_s(x)$, and the corresponding zero-crossings correspond to the transformation of the inflexion points in $f * \theta_s(x)$. The reasoning for this method is that the crossings through zero correspond to the most significative characteristics in the iris region.

- **Haar Wavelets**

  Lim et al. [74] also uses a wavelet transform to extract the iris characteristics. This time, the method uses a multidimensional filtering, which computes a characteristic vector of 87 samples. Since each component of this vector is a real value between $[-1, +1]$, the vector will be quantified with a sign: any positive value will be represented with 1, and 0 will denote a negative value. This results in a compact 87 bits biometric template. Lim et al. compares the use of Gabor filters and Haar transform and shows a 0,9 % improvement of the results when using Haar wavelets.

Discrete Cosine Transform (DCT)

Monro et al. [75] uses the DCT for feature extraction. The DCT is applied to overlapping rectangular image patches, rotating the image 45° from the radial axis. Differences between the DCT coefficients of adjacent patch vectors are computed and a binary code is created from their crosses through zero. To speed up the matching process, only the three most prominent binarized DCT coefficients are used, discarding the rest of them.

4.8.3. Non binary (real-valued) feature vector

This group of feature extraction methods focuses on representing the iris texture with a real-valued feature vector instead of a binary vector. This is the approach used by Wildes et al. [36], who decomposes the iris region with Laplacian of Gaussian filters to define the iris pattern. These filters are defined as:

$$\nabla G = -\frac{1}{\pi\sigma^4}\left(1 - \frac{\rho^2}{2\sigma^2}\right) \cdot \exp\left(\frac{-\rho^2}{2\sigma^2}\right) \tag{4.21}$$

where σ is the gaussian standard deviation and ρ is the radial distance of a point of the filter center.

The filtered image is then represented as a Laplacian pyramid that can compress the data and keep only the significant information. Wildes creates a 4-level pyramid, each level with a different resolution. Although this pyramid is efficient to create a compact pattern, a more detailed Laplacian pyramid is defined by Burt and Adelson in [76].

As with the binary-based methods, there are also many studies that have made use of various wavelets, but rather than using the output of the wavelet transform to create a binary feature vector, the output is kept as a real-valued feature vector. Examples include [77, 78]. Other major trend makes use of statistical methods for feature extraction, such as Independent Component Analysis (ICA) or Principal Component Analysis (PCA) [79].

4.9. Matching Algorithms

4.9.1. Introduction

All of the feature extraction algorithms presented before give as a result a sequence of numbers or a pattern that, by themselves, give no information about their relation with the templates stored in the database. Once the features have been extracted, a pattern matching procedure is done, which can be divided in:

1. *Evaluation of the similarity* with the stored information, resulting in a similarity score.
2. *Recognition decision*: acceptance/rejection of the user.

In general, the second stage is based on a threshold that regulates the acceptance/rejection decision. The level of security that the application requires will make its value more or less strict, increasing the number of false rejections or the false acceptances accordingly.

The most used iris matching algorithms are summarized next.

Hamming Distance

The *Hamming Distance* (HD) is defined as the number of bits that are different between two binary vectors. Therefore, it measures the similarity between two strings of equal length. Given two vectors X and Y of N samples, the Hamming distance is defined as:

$$HD = \frac{1}{N}\sum_{j=1}^{N} X_j(\mathbf{XOR})Y_j \tag{4.22}$$

The Hamming distance was originally conceived for detection and correction of errors in digital communication. In the context of model checking, the minimum Hamming distance is used as an evaluation of similarity. If two extracted feature vectors have a Hamming distance close to 0, they probably belong to the same user. For two independent iris patterns, for example the feature vectors extracted from the acquisition of two different irises, the obtained Hamming distance will be close to 0,5. The reason for this is that the independence of the patterns makes the string of bits completely random [63].

Daugman uses this measure in his iris recognition system. The literature gathers different applications and modifications of this technique. For example, in [61], two noise masks, Xn and Yn are included in the previous formula to account for invalid bits. These bits can correspond to eyelashes or eyelids, which can be discarded from the calculations as follows:

$$HD = \frac{\sum_{j=1}^{N} X_j \ (\mathbf{XOR}) \ Y_j \ (\mathbf{AND}) \ Xn_j \ (\mathbf{AND}) \ Yn_j}{N - \sum_{k=1}^{N} Xn_k \ (\mathbf{OR}) \ Yn_k} \tag{4.23}$$

Weighted Euclidean Distance

The *Weighted Euclidean Distance* (WED) gives a measure of how similar two different set of values are. The simplest interpretation of this measure is the distance between two points that one would measure with a ruler. The closer they are, the more similar. It is very uselful to compare two templates, especially if they are made of integers. In [80] Zhu et al. used this distance, defined as:

$$WED(k) = \sum_{i=1}^{N} \frac{(f_i - f_i^k)^2}{(\sigma_i^k)^2} \tag{4.24}$$

where f_i is the i^{th} characteristic of the unknown iris, f_i^k is the i^{th} characteristic of the iris template, k, and σ_i^k is the standard deviation of the i^{th} characteristic of the unknown iris k.

Correlation

The *correlation* is another measure of similarity between two patterns, defined as follows:

$$C = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} (p_1[i,j] - \mu_1) \cdot (p_2[i,j] - \mu_2)}{\sigma_1 \sigma_2} \tag{4.25}$$

where p_1 and p_2 are two images of $n \times m$ size, μ_1 and σ_1 and the mean and standard deviation of p_1, and μ_2 and σ_2 are the mean and standard deviation of p_2. A slightly modified version of this distance is the one chosen by Wildes et al. in [24] to compare real vectors (not binary) iris representations. In his system, Wildes uses the normalized correlation to avoid local intensity variations in the image, which is defined as:

$$NC = \frac{\sum_{i=1}^{n} \sum_{j=1}^{m} (p_1[i,j] - \mu_1) \cdot (p_2[i,j] - \mu_2)}{nm \sigma_1 \sigma_2} \tag{4.26}$$

4.10. Vulnerabilities of iris recognition systems

Biometrics appeared as an answer for the increasing need of a correct assessment of identity. Its main advantage is that they are based on something that the individual *is* rather than something he *knows* (like a password or a PIN) or something he *has* (like a key or token). But at the same time, this represents a terrible threat to the system robustness. A forgotten password can be easily regenerated, just as a lost key can be restored. However, a biometric trait cannot be replaced if an impostor "steals" it. Also the accessibility and lack of secrecy of this features (everyone knows our face and could get our fingerprints) raises security concerns.

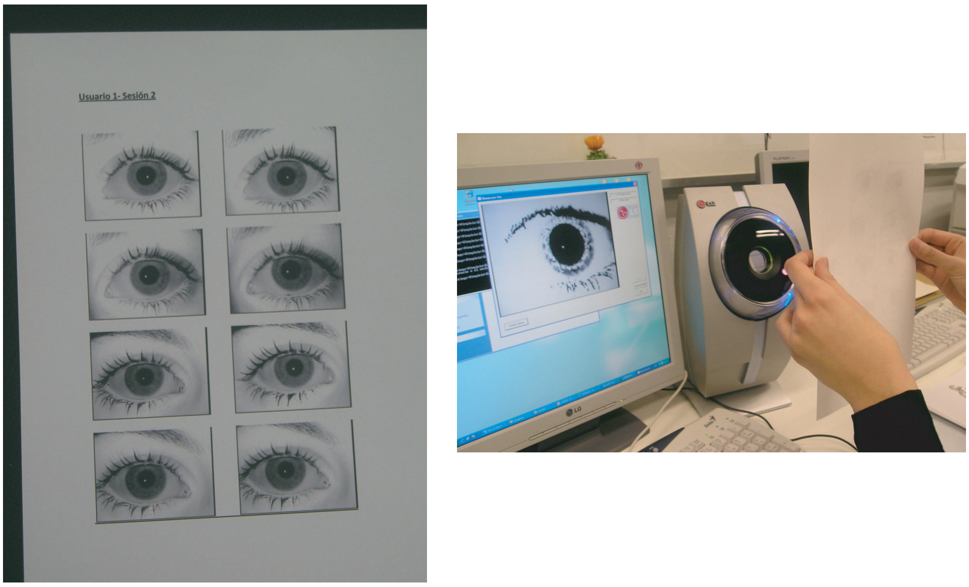


Figure 4.25: Fake iris capture.

As it has been exposed in Sec 3.3.5, there are eight different points of attack to a biometric verification system. In the present work we have concentrated our efforts in studying direct attacks on iris-based verification systems. These attacks focus on recreating artificial irises through printed images or even eye contact lenses and presenting them to the system. One of our own studies [14] pre-processed and printed the original images before presenting them at the iris sensor and acquiring them, as shown in Figure 6.11.

As we will see in the experimental section, iris recognition systems are highly vulnerable to these attacks. However, their success will be threatened in case that the system had human supervision.

Literature already offers a number of different solutions to this problem. One of the most popular is the use of liveness detection procedures. For the case of iris recognition systems, light reflections or pupil response to a sudden lighting event have been proposed [81, 82]. A person's unique reflex response could also be used as a characteristic feature, as proposed by Nishigaki et al. [83]. By using the eye's blind spot, they induce saccades, which are the repeated, tiny, left-to-right movements of the eye. Each pattern of responses would be unique to the individual. Since reflexes, by their very nature, are beyond conscious control, even when they are revealed they would be very difficult to spoof. This is a transformation of identification from differences in physiological biometric information into differences in human reflexes.

4.11. Weaknesses and challenges

Despite the great improvements made in this field over the past years, there are still some issues that need to be reviewed.

4.11.1. New non-invasive capturing techniques

Iris on the move leads the new trend for iris image acquisition. This technique aims for a more user-friendly iris capture based on videos. Once the face has been localized with a lower resolution camera, a more powerful one will be the one in charge of eye recognition. The main advantages of this method are the very low personal intrusivity required for the image acquisition and that the system can be used in real time. There are a number of prototypes that are being developed, like the one presented by Matey Group from Sarnoff Corporation [28].

4.11.2. Eyelashes and eyelids detection and removal

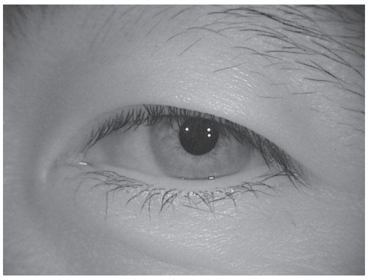


Figure 4.26: Example of Asian feature acquisition

Although the variability in the image acquisition for iris-based systems is much less than for other biometric traits (for example, the face), this biometric needs to deal with the world differences of this human feature. For example, Asian people have generally a less visible iris pattern whereas Occidentals have usually longer eyelashes that may disturb the obtained pattern, as shown in Figure 4.26. Therefore, different proposals have been presented to cope with this issue.

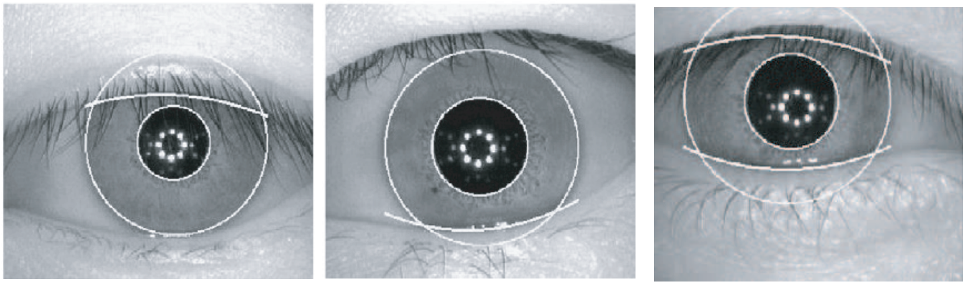


Figure 4.27: Process of estimation and isolation of eyelash occlusion

One of them was proposed by Basit et al. in [84] and is shown in Figure 4.27. This method simply traces a curved line along the eye, as tight as possible to define the eyelashes and eyelid region. This is a very effective way to separate iris from the rest, although it wastes too much useful information.

To overcome this problem, another solution was proposed in [85]. This second method is based on eyelashes detection through thresholding. First, the region of possible eyelashes is estimated, and in this area they will be isolated and not taken into account for feature extraction. An example of this process is shown in Figure 4.28.

4.11.3. Segmentation improvements

As it has been presented, iris segmentation branches off in many different directions. Current investigations take different paths, looking for the most reliable solution. One of the new techniques is the pupil manipulation and search of non-correctly identified boundaries. The main

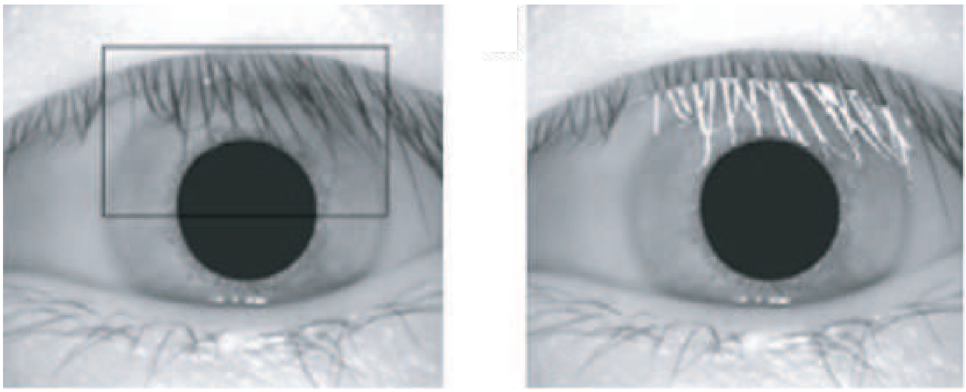


Figure 4.28: Optimized eyelash isolation process

reason for this error is off-angle captures like the one shown in Figure 4.29, which lead to non circular pupils.

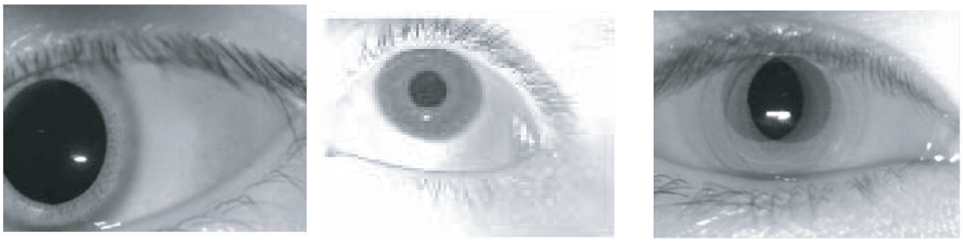


Figure 4.29: Non-ideal iris captures

Another line of investigation deals with image occlusion, in Figure 4.30, due to eyelashes, eyelids or specular reflections. In extreme situations, it will not be possible to process the iris image, and it will be discarded. A third subject of study is the obtention of a robust and reliable segmentation of the iris pattern from users with glasses or contacts lens.

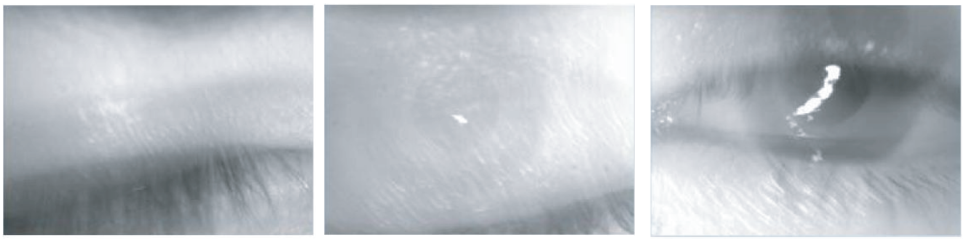


Figure 4.30: Occluded iris captures

4.11.4. Image quality measures

One of the problems that biometric systems have to deal with is whether an image is good enough to be used for recognition. This issue is especially relevant during the enrollment process, since a weak or erroneous stored template can be a security hole and may prevent the user from entering the system in posterior accesses. Different studies point out the benefits of using an image quality indicator to improve the system performance [86, 87]. However, there is not a general agreement on a system that can determine the image quality with total certainty.

4.12. Competitions and evaluations of iris recognition

The Iris Challenge Evaluation (ICE) [88] was a project conducted by the National Institute of Standards and Technology (NIST [89]), which organized large-scale, open and independent technology evaluations for iris recognition. The ICE emerged with the need of an evaluation to measure the accuracy of the underlying technology that makes iris recognition possible.

The goals of the ICE were:

- To promote the development and advancement of iris recognition.
- To assess the technology's current level of performance.

The ICE evaluation was composed of two editions in 2005 and 2006. The first edition seeked researchers and developers from industry to participate in iris recognition "challenge problems". These problems tried to promote technology development and give the participants the opportunity to improve their performance rates. On the second edition, a large-scale, independent evaluation was scheduled. Iris matching performance was evaluated against newly captured images to guarantee an accurate assessment, and a standard dataset and test methodology were employed for an even evaluation. Carnegie Mellon University, CASIA and Iridian Technologies, Inc. were among the 8 organizations from 6 Countries which took part in this evaluation.

The ICE was sponsored jointly by the following federal agencies: NIST; two Department of Homeland Security agencies–the Science and Technology Directorate and the Transportation Security Administration; two Department of Justice agencies–the Federal Bureau of Investigation and the National Institute of Justice; the Intelligence Technology Innovation Center under the Office of the Director of National Intelligence; and the interagency Technical Support Working Group, the U.S. national forum that identifies, prioritizes and coordinates interagency and international research and development requirements for combating terrorism.

The Noisy Iris Challenge Evaluation (NICE) is a contest which focuses on the study and development of less constrained iris recognition systems and in the visible wavelength. The ICE competition evaluated systems under too perfect conditions, and did not simulate a real iris recognition environment. This is how NICE came about. Its main goal is to evaluate the robustness to noise of iris segmentation and noise detection algorithms toward iris recognition. It operates on the highly noisy data of UBIRIS. V2 database, where noise factors are induced.

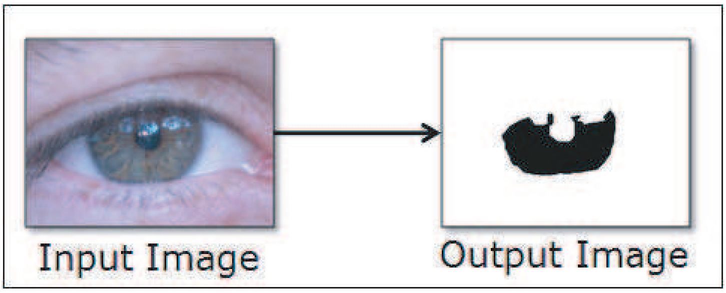


Figure 4.33: NICE I fundamental task

It is divided in two phases that together perform a complete evaluation of the most traditional stages of iris recognition systems. The first part (NICE I in 2008) is focused on the segmentation and noise detection of the iris images captured (Figure 4.33), distinguishing between the regions of the iris. The 8 methods that showed the best performance were published in a special issue of the Image and Vision Computing Journal (IVC). The complementary part which is evaluated in the NICE II edition in 2010 (currently underway) comprises the encoding and matching of previously segmented noisy images. Once more, the 8 methods which achieve the lowest error rates are invited to publish their approach in the Pattern Recognition Letters Journal.

4.13. Databases

Database	**Num. of iris**	**Num. of images**	**Capturing device**	**Source**
CASIA1	108	756	CASIA camera	Download from: http://www.cbsr.ia.ac.cn/english/Databases.asp
CASIA3	1500	22051	CASIA camera and OKI irispass-h	
ICE2005	244	2953	LG2200	E-mail: ice@nist.gov
ICE2006	480	60000	LG2200 camera	
MMU1	90	450	LG IrisAccess camera	Download from: http://pesona.mmu.edu.my/∼ccteo/
MMU2	199	995	Panasonic BM-ET100US Authenticam	E-mail: ccteo@mmu.edu.my
UBIRIS	241	1877	Nikon E5700	Download from: http://iris.di.ubi.pt/ubiris1.html
Univ. Bath	800	16000	ISG LigthWise LW-1.3-S-1394	See: http://www.bath.ac.uk/ elec-eng/research/sipg/irisweb/database.htm
UPOL	128	384	SONY DXC-950P 3CCD	Download from: http://phoenix.inf.upol.cz/iris/
WVU	488	3099	OKI irispass-h	E-mail: arun.ross@mail.wvu.edu
BioSec	400	3200	LG IrisAccess 3000	See: http://atvs.ii.uam.es/databases.jsp
BioSecurID	800	12800	LG IrisAccess 3000	

Table 4.4: Main current iris databases.

With fast development of iris image acquisition technology, iris recognition is expected to become a fundamental component of modern society. However, performance of iris recognition systems in unconstrained environments is still far from perfect. The success of investigations often depends on the availability of carefully designed iris image databases of sufficient size. Such publicly available datasets are however very limited. In Table 4.4 the most popular iris databases available are presented.

5
System, design and development

Scale Invariant Feature Transformation (SIFT) was developed by Lowe [2] as an algorithm capable of detecting stable feature points in an image. These points are invariant to image translation, scaling, rotation, illumination and affine image transformations. It was originally developed for general purpose object recognition and it performs matching based on the descriptor representing each feature point. In this work, we implement the Scale Invariant Feature Transformation (SIFT) for its use in biometric recognition using iris images. One of the main advantages of using the SIFT technique is that there is no need to transform the feature points into polar coordinates. When converting an iris region to polar coordinates, it is necessary a very accurate segmentation in order to create a similar iris pattern mapping between images of the same eye, which can fail with non-cooperative or low quality data (e.g. changes in the eye gaze, non-uniform illumination, eyelashes/eyelids occlusion, etc.). Instead of the traditional image segmentation and filtering, SIFT uses *difference of Gaussian (DoG)* to locate points in the ring-shaped iris image directly and then describe these feature points by the relative gradient orientation of the feature point compared with surrounding points within some window size. Therefore, the main differences between traditional iris recognition approaches and the SIFT technique are: i) there is no need to transform the iris region to polar coordinates, avoiding the inherent problems of this procedure with non-ideal images; and ii) the features used for recognition are extracted from local distinctive regions only (i.e. points), rather than encoding the whole iris region. In order to reduce the computational cost of extracting these features, a cascade filtering approach is used, in which the more expensive operations are applied only at the points that pass less consuming processes.

The SIFT algorithm mainly is comprised of four stages described in this section following Lowe's implementation [2]. These four basic steps are:

1. **Scale-space extrema detection**: The first step of the algorithm performs a search over all scales and locations of the image to identify potential points of interest, invariant to scale and orientation. It is done by using the DoG (*Difference-of-Gaussian*) function.

2. **Keypoint localization**: In order to find accurate *keypoints*, an stability measure is applied, so non-suitable candidate points are discarded.

3. **Orientation assignment**: Based on local image gradient directions, one or more orientations are assigned to each extracted keypoint location. All future operations are performed on data transformed relative to the assigned orientation, scale, and location, thereby providing invariance to these transformations.

4. **Keypoint descriptor**: The last step results in a representation of the keypoints, as a measure of the local image gradients at the selected scale in the region around them. Each feature point corresponds to a feature vector composed of 128 elements. As it will be seen, this representation gives a partial invariance to shape distortion and illumination changes.

The stability of feature points is important since comparison of two objects from different images is dependent on the comparison of the same feature points. To ensure the most stable points, Brown and Lowe [90] propose a 3D function to remove points located along edges or with low contrast, which are more susceptible to noise. The SIFT method has been widely used for object recognition applications, and has been recently proposed for its use in biometric recognition systems based on face [10, 11], fingerprint [12], and iris images [8].

Figure 5.1 shows a diagram of the recognition system implemented in this Project using the SIFT operator.

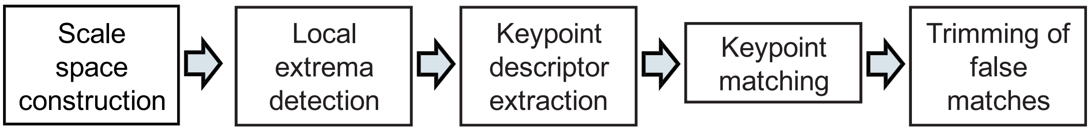


Figure 5.1: Steps of the SIFT operator for iris matching.

5.1. Scale-space local extrema detection

This first stage aims to obtain a number of candidate points in the image which can be repeatedly identified under different views of the same object. The SIFT detector and descriptor are constructed from the Gaussian scale space of the source image, in which one can efficiently detect stable key point locations, invariant to scale changes of the image. The Gaussian scale space $L(x, y, \sigma)$ of an image is defined as the convolution of 2D Gaussian functions $G(x, y, \sigma)$ of varying widths σ with the input image $I(x, y)$:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \tag{5.1}$$

where (x, y) are the spatial coordinates and σ is the scale factor.

The algorithm makes use of the *Difference of Gaussian* (DoG) function, which is, coarsely speaking, the scale derivative of the Gaussian scale space. The DoG function $D(x, y, \sigma)$ is obtained by subtracting subsequent scales in each octave:

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \tag{5.2}$$

were k is a constant multiplicative factor in scale space. The DoG are used for several reasons. First, it is an efficient function which requires low computational power to compute: The smoothed images $L(x, y, \sigma)$ need to be computed for scale space feature description and therefore, D can be computed by simple subtraction. Furthermore, Mikolajczyk [91] found that the maxima and minima of scale-normalized Laplacian of Gaussian produce the most stable image features compared to other possible image functions such as the gradient, Hessian or Harris corner function, and the scale-normalized Laplacian of Gaussian can be approximated by the DoG.

The set of Gaussian-smoothed images and DoG images are called an octave. A set of such octaves is constructed by successively down sampling the original image by a factor of 2. Each octave (i.e., doubling of σ) is further subdivided into an integer number of sub-levels or scales s. The distinction between octave and scale is important because at each successive octave the

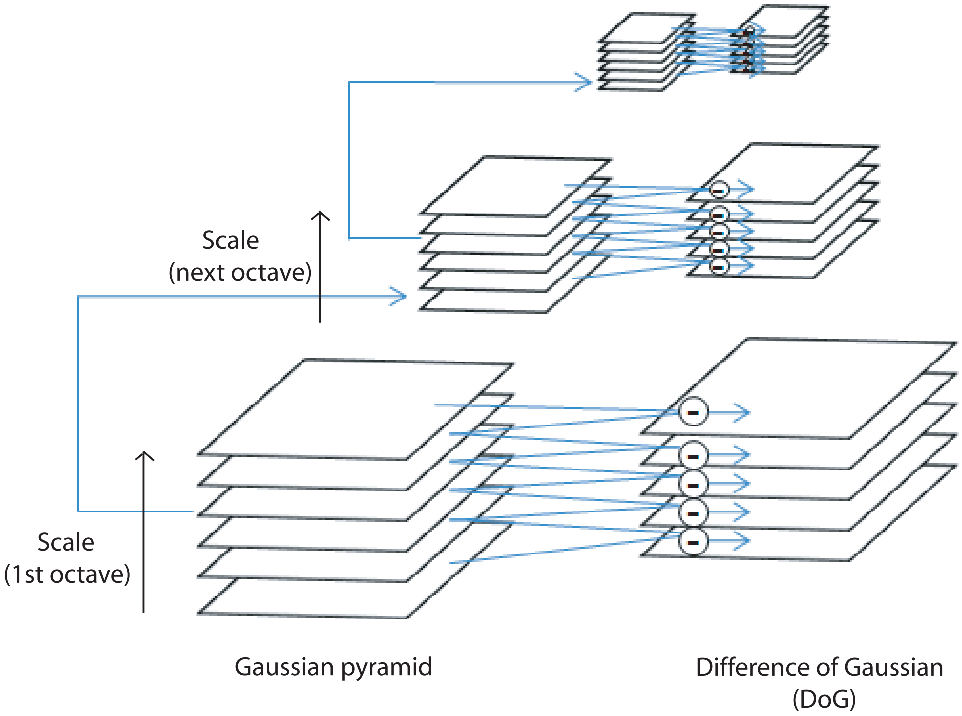


Figure 5.2: The original image convolved with Gaussians gives the Gaussian pyramid on the left. Each neighboring octave is separated by a constant scale factor. Adjacent Gaussian images are substracted to create the Difference of Gaussian images on the right. The Gaussian image with σ twice that of the initial value is down-sampled by 2 and used to construct the next octave.

data is spatially down sampled by half, so $k = 2^{1/s}$. Once a complete octave has been processed, the first image in the next octave is created by subsampling the image of the previous octave which has twice the initial value of sigma (it will be two images from the top of the octave). This greatly improves the efficiency of the algorithm at lower scales. The process is shown in Figure 5.2. To make full use of the input image, the image is expanded to create more sample points that were present in the original. Therefore, the size of the input image is doubled prior to building the first level of the pyramid.

Since the scale space $L(x, y, \sigma)$ represents the same information at different levels of scale, this particular way of image sampling allows us to reduce redundancy. Therefore s+3 images for each octave must be produced, so that the final extrema detection covers a complete octave (in order to form s+2 DoG images). In this project we have used s=3, which is the frequency of sampling in scale that gives the highest repeatability according to Lowe's studies. It has been proved that repeatability does not improve as more scales are sampled because extrema that are close together are much more unstable to small changes of the image. Hence, this extrema are less likely to be detected in the transformed image. However, with increased sampling of scales, the number of key points rises since the extrema can be arbitrarily close together (no minimum spacing of samples that will detect all extrema is determined) and so it does the total number of correct matches. As it has been mentioned before, this method was originally developed as an object recognition technique, and so, a large number of correctly matched features is more valuable than an error free matching but with very few extracted characteristic points. Therefore, it will be optimal to use a large number of scale samples, although the cost of computation also rises with this number. The chosen number of scales is therefore a compromise between efficiency and completeness: although incomplete, it allows us to detect the most stable and useful features of the image with a reasonable frequency of sampling in scale.

In sum, six Gaussian-smoothed images and five DOG images per octave are produced. The other parameter which needs to be determined is the sampling relative to the scale of smoothing. Following Lowe's experiments it can be seen that this time repeatability continues to increase with larger frequency of sampling in the spatial domain (σ). Following a similar compromise between rate and detection and due to the computational cost, a value of σ=1.6 has been used. Both these values are the ones used in Lowe's implementation and a deeper explanation can be found in [2]. Figure 5.3 shows 3 successive octaves with 6 scales and the corresponding difference images.

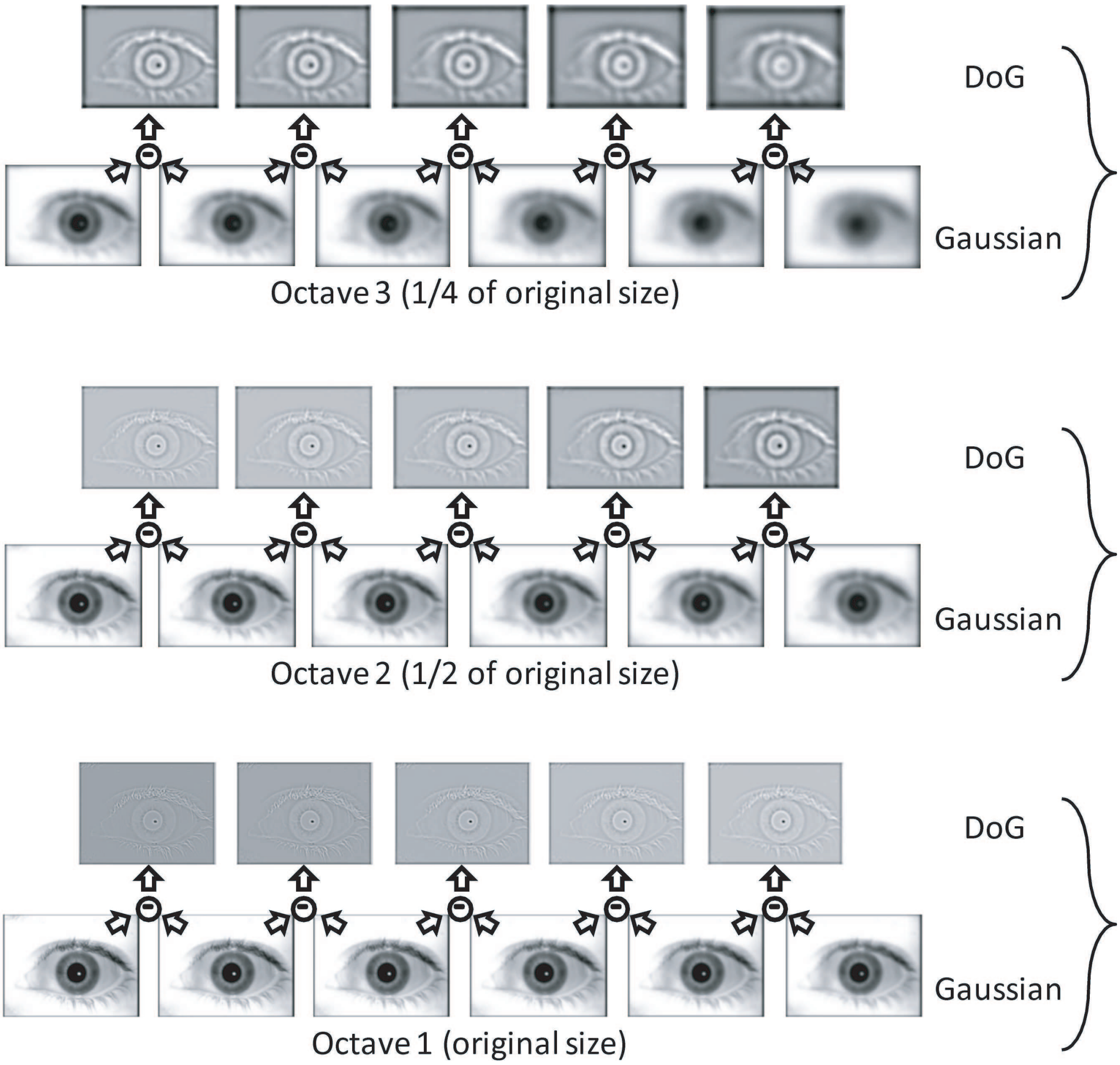

DoG
Gaussian
Octave 3 (1/4 of original size)
DoG
Gaussian
Octave 2 (1/2 of original size)
DoG
Gaussian
Octave 1 (original size)

Figure 5.3: Example of SIFT scale space construction. The figure shows 3 successive octaves, with 6 scales per octave, and the corresponding difference images.

Local extrema are then detected by observing each image point in $D(x, y, \sigma)$. A point is decided as a local minimum or maximum when its value is smaller or larger than all its surrounding neighboring points. This is, each sample point in $D(x, y, \sigma)$ is compared to its eight neighbors in the current image and the nine neighbors in the scale above and below, as shown in Figure 5.4. The computational cost of this step is reasonably low as many of the points in D(x,y,sigma) can be discarded when adjacent points are checked.

5.2. Accurate Keypoint Localization

Once a keypoint candidate has been found, it is analyzed to check its stability. Points with low contrast or situated along an edge are very sensitive to noise and cannot be reliably detected again with small variation of viewpoint or lighting changes in the image. Although further

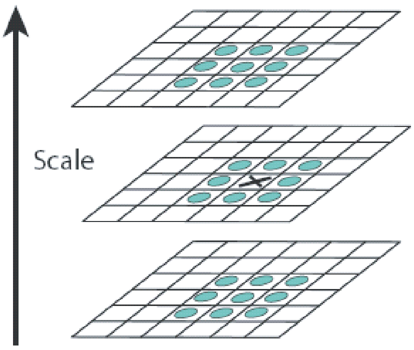


Figure 5.4: Maxima and minima of the difference-of-Gaussian images are detected by comparing a pixel (marked with X) to its 26 neighbors in 3×3 regions at the current and adjacent scales (marked with circles). Source: David Lowe [2].

restrictions (inherent to the operation of biometric systems) will be imposed to the candidate feature points during the experiments, the general system described by Lowe uses two criteria: one to exclude low contrast points and other to exclude edge points.

To eliminate low contrast extrema, a minimum threshold D is applied to the candidate points. Only those points above the threshold would be considered stable enough to be passed to the next step. However, we have noted that the threshold D indicated by Lowe discards too many SIFT keypoints of the iris region (Lowe uses D=0.03 when pixel values are in the range [0,1]). Thus, the optimal value of D to be used in our iris recognition system has been obtained experimentally. More details of this procedure are included in the experimental section.

To assure stability, poorly localized extrema (along edges) must also be discarded since they will be very unstable even when dealing with small amounts of noise. To do so, one can use the knowledge that the DoG functions have strong responses along edges. For true edges, the principal curvature is huge along the edge direction. On the other hand, the principal curvature is small along the direction perpendicular to the edge direction. These peak responses can be found through a Hessian matrix **H**, computed at the location and scale of the keypoint:

$$\mathbf{H} = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix} \tag{5.3}$$

where D is the second partial derivative of the DoG image $D(x, y, \sigma)$ at a scale s. The derivatives are estimated by taking differences of neighboring sample points. Through this square matrix one can describe the local curvature of the function. It can be demonstrated that the following inequality allows to find edge points:

$$\frac{Tr\,(\mathbf{H})^2}{Det\ \mathbf{H}} = \frac{(D_{xx} + D_{yy})^2}{D_{xx} \times D_{yy} - (D_{xy})^2} < \frac{(r+1)^2}{r} \tag{5.4}$$

Then, extrema points not fulfilling this inequality are discarded (a value of r=10 is used in this Project, according to the original paper [2]). After rejecting unstable edge points, the remaining extrema points can be assigned a descriptor.

5.3. Orientation assignment

The main characteristic of the SIFT features is that they are invariant to a series of image transformation. Invariance to image rotation can be achieved by assigning each of them a consistent orientation based on local image properties and representing they keypoint descriptor relative to this orientation. For each image sample within a 16×16 region around each keypoint, the gradient magnitude, m, and its orientation, θ, are computed using pixel differences:

$$m\left(x,y\right)=\sqrt{\left(L\left(x+1,y\right)-L\left(x-1,y\right)\right)^{2}+\left(L\left(x,y+1\right)-L\left(x,y-1\right)\right)^{2}} \tag{5.5}$$

$$\theta\left(x,y\right)=\arctan\frac{L\left(x,y+1\right)-L\left(x,y-1\right)}{L\left(x+1,y\right)-L\left(x-1,y\right)} \tag{5.6}$$

By choosing the Gaussian smoothed image, L, with the closest scale to the scale of the corresponding keypoint, the computations of the gradient of the points result invariant to scaling. An orientation histogram of 36 bins is formed from the gradient orientations, each including 10 degrees in order to cover the 360 degree range of orientations. Each sample added to the histogram is weighted by its gradient magnitude and by a Gaussian-weighted circular window centered at the keypoint. The purpose of this Gaussian window is to give less emphasis to gradients that are far from the center of the local extremum. The Gaussian window is designed such that its σ is 1.5 times that of the scale of the keypoint. Thus, each value of each bin in the histogram holds the magnitude sums from all the weighted points within that orientation.

The bin with the highest magnitude is selected as the dominant orientation. This peak corresponds to the dominant direction of local gradient. However, it is possible that there is more than one dominant direction. Any other local peak that is within 80 % of the highest peak will also be considered as a dominant direction. Therefore, for locations with multiple peaks, there will be multiple keypoints created at the same location, but with different orientations. Points with multiple orientations are not very common but add a significant stability in the matching step. For better accuracy, a parabola is fit to the 3 histogram values closest to each peak to interpolate the peak position. The major orientations of the histogram are then assigned to the keypoint so the keypoint descriptor are represented relative to them.

5.4. Keypoint descriptor

The previous operations have assigned an image location, scale, and orientation to each keypoint, thus providing invariance to these parameters. In this stage, a descriptor is computed for the local image region that is as distinctive as possible at each keypoint, yet as invariant as possible to remaining image variations (e.g. change in illumination or 3D viewpoint). The SIFT descriptor of a keypoint is a local statistic of the orientations of the gradient of the Gaussian scale space. The image gradient magnitudes and orientations, relative to the major orientation of the keypoint, are sampled within a 16×16 region around each keypoint. The process is similar to the one performed in the previous step. Each added sample will be weighted by its gradient magnitude and a Gaussian circular window. A Gaussian weighting function is used once more to avoid sudden changes in the descriptor with small changes in the position of the window, and give less emphasis to gradients that are far from the keypoint, as these are most affected by misregistration errors. The Gaussian σ is set to be 1.5 times the width of the descriptor window, forcing a smooth fall off across the window. To improve the efficiency of the algorithm, all the gradients are precomputed for all the levels of the Gaussian pyramid and can be seen in Figure 5.5 (*bottom left*) represented as small arrows.

Samples in the 16×16 window are accumulated into orientation histograms summarizing the contents over 4×4 subregions. Each orientation histogram has 8 bins, corresponding to 8

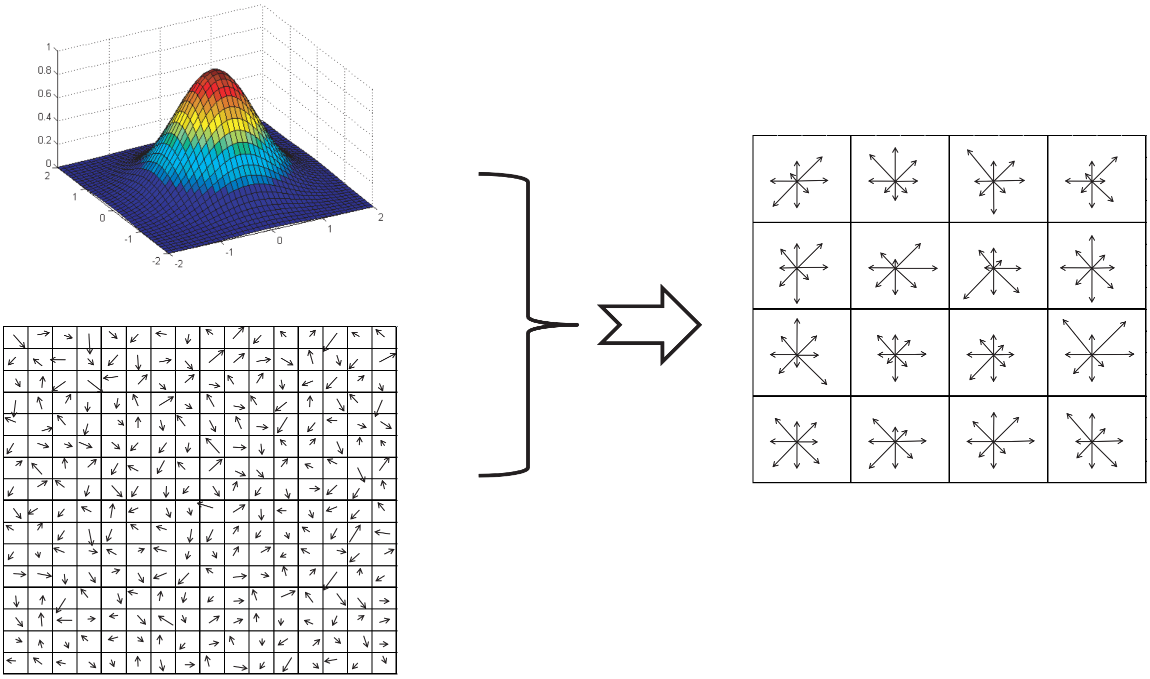


Figure 5.5: Computation of SIFT keypoint descriptor. The gradient magnitude and orientation at each image sample point in a region around the keypoint location is first computed, as shown on the left bottom, weighted by a Gaussian window shown on the left top. These samples are then accumulated into orientation histograms summarizing the contents over 4×4 subregions, as shown on the right, with the length of each arrow corresponding to the sum of the gradient magnitudes near that direction within the region.

directions, which cover the 360 degree range of orientations. Therefore, 16 histograms will be obtained for each keypoint as shown in Figure 5.5 (*right*), the length of each arrow corresponding to the magnitude of that histogram entry. By creating orientation histograms in 4×4 subregions we allow for significant shift in gradient positions. The representation of a descriptor by a vector containing the orientations around the keypoint location simulates the complex cell model with which the 3D recognition of biological vision is explained. This model outperforms in accuracy any correlation based model and allows for positional shifts. Therefore, the implementation of this shift can be understood by realizing that two samples that are 4 positions apart still contribute to the same histogram, allowing for a larger local positional shift.

The descriptor is then formed from a vector containing the values of all the orientation histogram entries. The descriptor is characterized by the number of subregions created around the keypoint (number of histograms) and also by the number of orientations per histogram (number of bins that each histogram contains). Therefore in our implementation there is a 4×4×8=128 elements feature vector for each keypoint. Although the number of features per descriptor might seem high, it has been proved that it performs better than lower-dimensional descriptors. One may think that a higher number of elements in the vector might improve the results. However a larger descriptor can actually hurt the matching process, since descriptors become more sensitive to noise and distortions. In short, a feature point is described by its relationship to its surrounding points.

The feature vector is modified to finally reduce the effects of illumination change. Illumination changes mainly affect the gradient magnitudes rather than the orientation. Therefore, our goal is to represent the gradient to minimize this error. First, the vector is normalized to unit length. A change in image contrast (pixels multiplied by a constant) will be canceled by this normalization, whereas changes in brightness (a constant added to each pixel) will not affect the gradient values (computed as pixel differences). However, this normalization would only palliate the effects of affine illumination changes. Changes due to capture effects or device artifacts would affect the image in a non-linear way and can cause large changes in relative magnitudes for the gradient (e.g. camera saturation). One can reduce this large magnitude impact by thresholding the values of the feature vector and renormalizing it. For this purpose, a threshold value of 0.2 is used, according to Lowe's guidelines [2].

5.5. Keypoint matching

Matching is performed by comparing each local extrema based on the associated descriptors. Suppose we want to match two images I_1 and I_2. The best candidate match for each keypoint in I_1 is found by identifying its nearest neighbor in the set of keypoints from I_2. The nearest neighbor is defined as the keypoint within minimum Euclidean distance for the previously described descriptor vector. Given a feature point p_{11} in I_1, its closest point p_{21}, second closest point p_{22}, and their Euclidean distances d_1 and d_2 are calculated from feature points in I_2. When the ratio d_1/d_2 is sufficiently small, then points p_{11} and p_{21} are considered to match. Then, the matching score between two images can be decided based on the number of matched points and geometric configuration. According to [2], we have chosen a threshold of 0,76 for the ratio d_1/d_2.

5.6. Trimming of false matches

For measuring the distinctiveness of features, it is important to know how reliable the matching is. The keypoint matching procedure described may generate some erroneous matching points. Also, it is possible that keypoints from an image may not have any correct match because they were occluded or not detected in the candidate images of the system database. There are different approaches for this problem. One of the most intuitive is to removed spurious matching points using geometric constraints [12] by limiting typical geometric variations to small rotations and displacements. Therefore, if we place two iris images side by side and draw matching lines as shown in Figure 5.6 (top), true matches must appear as parallel lines with similar lengths. According to this observation, we compute the predominant orientation θ_P and length ℓ_P of the matching, and keep the matching pairs whose orientation θ and length ℓ are within predefined tolerances ε_θ and ε_ℓ, so that $|\theta - \theta_P| < \varepsilon_\theta$ and $|\ell - \ell_P| < \varepsilon_\ell$. It must be stated that this procedure is not included in the original description of the SIFT method [2], but it is found in some application-oriented implementations like that found in [12]. This measure performs well because correct matches need to have the closest neighbor significantly closer than the closest incorrect match in order to assure reliable matching. The result of this procedure is shown in Figure 5.6 (bottom).

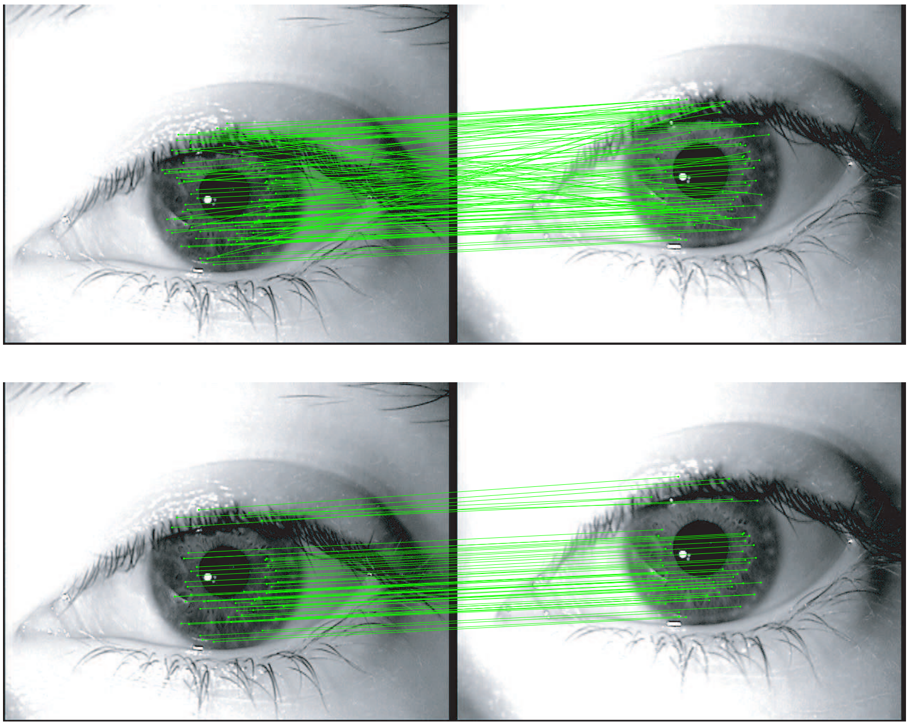


Figure 5.6: Matching of two iris images using SIFT operators without and with trimming of false matches using geometrical constraints (top and bottom, respectively). Trimming of false matches is done by removing matching pairs whose orientation and length differ substantially from the predominant orientation and length computed from all the matching pairs.

6

Experiments and Results

6.1. Database and Protocol

For the experiments of this Project, we use the BioSec baseline database [13]. It consists of 200 individuals acquired in two acquisition sessions, separated typically by one to four weeks. A total of four iris images of each eye, changing eyes between consecutive acquisitions, are acquired in each session. The total number of iris images is therefore: 200 individuals × 2 sessions × 2 eyes × 4 iris = 3,200 iris images. We consider each eye as a different user, thus having 400 users. Glasses were removed for the acquisition, while the use of contact lenses was allowed. The database have been acquired with the LG Iris Access 3000 sensor, (see Figure 6.1), with an image size of 640 pixels width and 480 pixels height. Some iris examples are shown in Figure 6.2.

Figure 6.1: LG Iris Access 3000 sensor.

The 200 subjects included in BioSec Baseline are further divided into [13]: *i*) the *development set*, including the first 25 and the last 25 individuals of the corpus, totaling 50 individuals; and *ii*) the *test set*, including the remaining 150 individuals. The development set is used to tune the parameters of the verification system and of the fusion experiments done in this Project (later indicated in this Section). No training of parameters is done on the test set. The following matchings are defined in each set: *a*) genuine matchings: the 4 samples in the first session to the 4 samples in the second session; and *b*) impostor matchings: the 4 samples in the first session to 1 sample in the second session of the remaining users. With the development set, this results in 50 individuals × 2 eyes × 4 templates × 4 test images $= 1,600$ genuine scores, and 50 individuals × 2 eyes × 4 templates × 49 test images $= 19,600$ impostor scores. Similarly, for the test set we have 150 individuals × 2 eyes × 4 templates × 4 test images $= 4,800$ genuine scores, and 150 individuals × 2 eyes × 4 templates × 149 test images $= 178,800$ impostor scores.

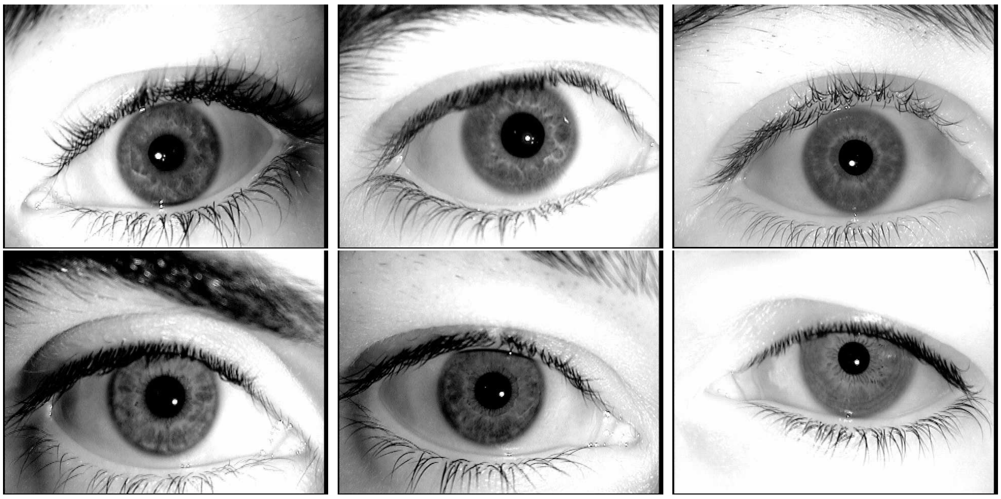


Figure 6.2: Iris examples from the BioSec database.

6.2. Iris Segmentation

We have automatically segmented iris images using circular Hough transform in order to detect the iris and pupil boundaries, which are modeled as two concentric circles. To improve the performance of this segmentation procedure, we pre-estimate the iris centroid by histogram thresholding, since iris region is observed to have the lowest gray levels of an iris image. This pre-estimation allows to reduce the searching area of the circular Hough transform. Also, we impose three conditions to the two circles that model iris and pupil boundaries: *i*) although these two circles are known to be non-concentric, a maximum value is imposed to the distance among their centers; *ii*) the two circles are not allowed to to have parts outside the iris image; and *iii*) the radius of the two circles are not allowed to be similar.

Then, automatically segmented images have been visually inspected to manually correct images not well segmented. With this procedure, we obtain a correct segmentation of the 100 % of the database. The objective is to avoid bias in the matching performance during the optimization of the SIFT iris recognizer due to incorrectly segmented images. We then construct a binary mask that includes only the iris region and use it to discard SIFT keypoints being detected outside the mask. An example of segmented images together with the detected SIFT keypoints can be seen in Figure 6.3. Since eyelash and eyelid occlusion is not very prominent in the BioSec database, no technique was implemented to detect eyelashes or eyelids.

6.3. Baseline Iris Matcher

In order to compare the performance of the proposed iris recognition system based on SIFT features, we use as baseline iris matcher the freely available[1] iris recognition system developed by Libor Masek [61, 92], which is based on the classical transformation to polar coordinates and Log-Gabor wavelets.

This system performs a normalization of the segmented iris region by using a technique based on Daugman's rubber sheet model [7], as described in Section 4.6. The centre of the pupil is considered as the reference point, and radial vectors pass through the iris region. Since the pupil can be non-concentric to the iris, a remapping formula for rescale points depending on the angle around the circle is used. Normalization produces a 2D array with horizontal dimensions of angular resolution and vertical dimensions of radial resolution, in addition to another 2D noise

[1] The source code can be freely downloaded from `www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html`

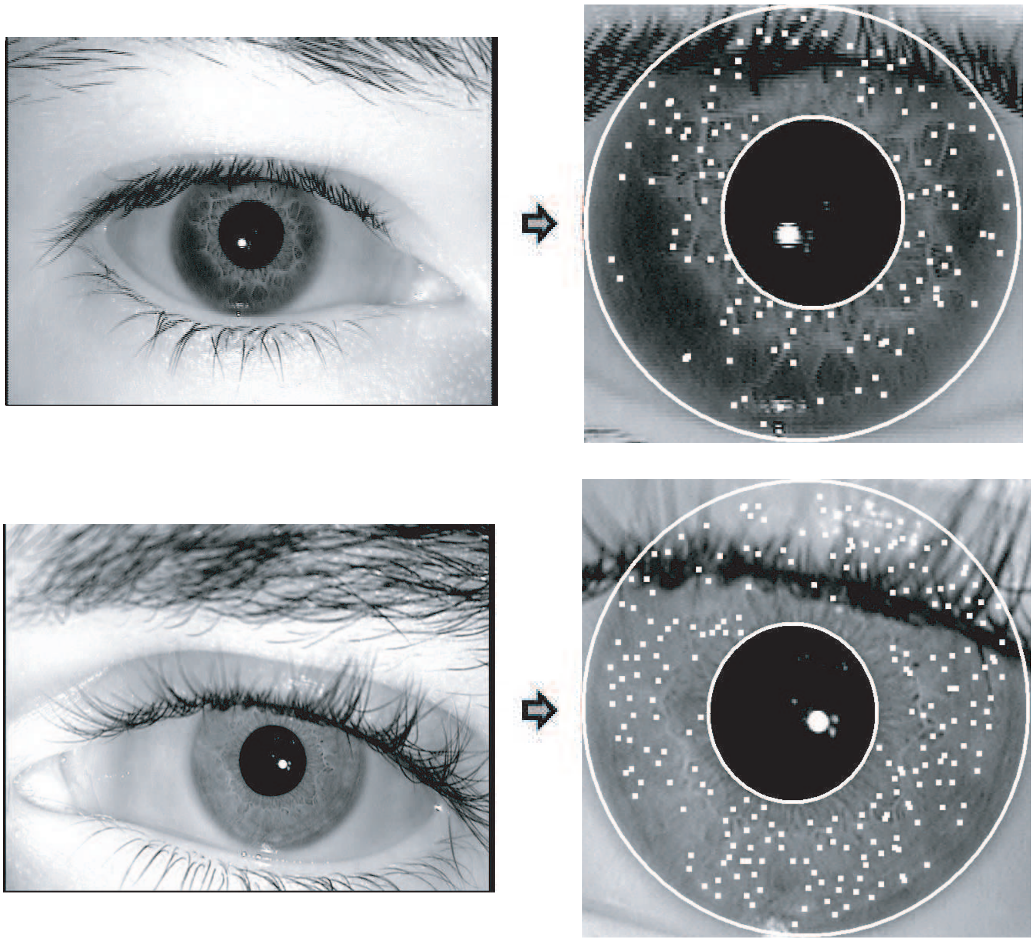


Figure 6.3: Example of segmented images together with their detected SIFT keypoints (no size doubling of the input image is done in this example).

mask array for marking reflections, eyelashes, and eyelids. This normalization step is as shown in Figure 6.4. Since we have computed SIFT features in the whole segmented iris region, we have deactivated the computation of the noise mask to make the comparison between the two systems fairer.

Feature encoding is implemented by convolving the normalized iris pattern with 1D Log-Gabor wavelets. The 2D normalized pattern is broken up into a number of 1D signals, and then these 1D signals are convolved with 1D Gabor wavelets. The rows of the 2D normalized pattern are taken as the 1D signal, each row corresponds to a circular ring on the iris region. It uses the angular direction since maximum independence occurs in this direction [61].

The output of filtering is then phase quantized to four levels using the Daugman method [7], with each filtering producing two bits of data. The output of phase quantization is a grey code, so that when going from one quadrant to another, only 1 bit changes. This will minimize the number of bits disagreeing, if say two intra-class patterns are slightly misaligned and thus will provide more accurate recognition [61]. The encoding process produces a bitwise template containing a number of bits of information.

The *Hamming distance* (HD) is chosen as the matching metric, since bitwise comparisons are necessary. In order to account for rotational inconsistencies, when the Hamming distance of two templates is calculated, one template is shifted left and right bitwise and a number of Hamming distance values is calculated from successive shifts [7]. This method corrects for misalignments in the normalized iris pattern, caused by rotational differences during imaging. The lowest computed distance value will be the one taken.

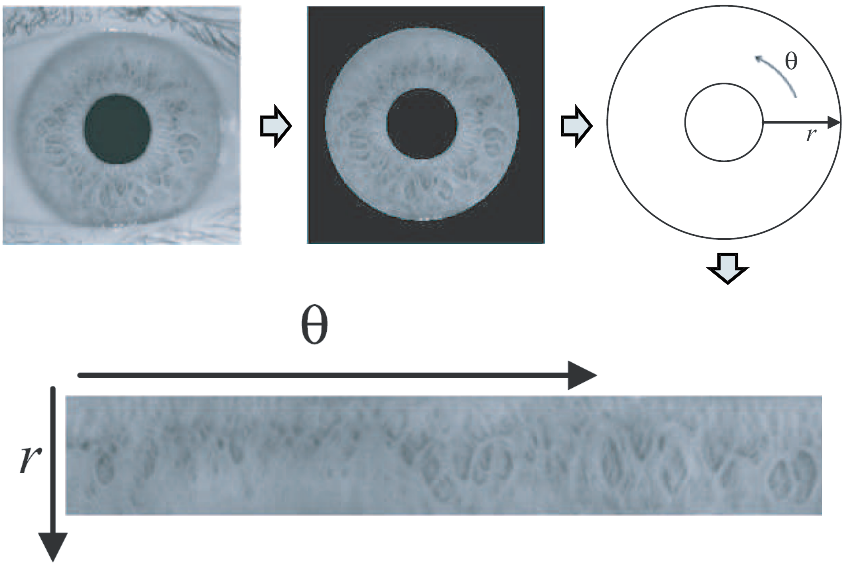


Figure 6.4: Normalization of the iris region to polar coordinates. The ring-shaped region of the iris is transferred to a rectangular image, with the pupil center being the center of the polar coordinates.

6.4. Experimental Results

The experimental tests carried out in this project are divided in two main sections. First, the SIFT method is optimized for the developed database and an evaluation and comparison to the reference system is conducted to estimate the performance of this work. The second part of the experiments involve a study of the vulnerability of the developed system to direct attacks.

6.4.1. Setting the Optimal Parameters

The SIFT matcher is optimized in terms of its different parameters. The experimental parameters to be set are: the scale factor of the Gaussian function σ=1.6; the number of scales s=3; the threshold D excluding low contrast points; the threshold r excluding edge points (r=10); the threshold of the ratio d_1/d_2 (set to 0,76) and the tolerances ε_θ and ε_ℓ for trimming of false matches. The indicated values of the parameters have been extracted from Lowe [2]. We have noted however that the threshold D indicated in [2] discards too many SIFT keypoints of the iris region (D=0.03 when pixel values are in the range [0,1]). Thus, together with ε_θ and ε_ℓ, we have decided to find an optimal value also for D.

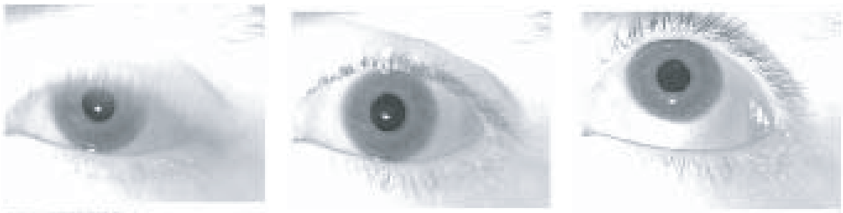


Figure 6.5: Iris images belonging to the same individual, that will most likely give a different number of SIFT points.

When matching two iris images, the matching score between them can be decided based on the number of matched SIFT points. However, this criterion does not reflect the fact that the two images may have a different amount of detected SIFT points, which can happen for example due to eyelashes/eyelids occlusion, changes in the eye gaze or illumination problems (see Figure 6.5), leading to useless iris parts. This is a common problem when the feature vector representing a biometric trait does not have constant size, as it is the case of our SIFT matcher, where the number of detected points between different iris images is not constant. Given two iris images, let p_1 and p_2 be the number of detected SIFT points on each, let NM be the number of matched points (with $NM \leq \text{mín}(p_1, p_2)$), and let $\mathbf{d} = [d_1, ..., d_{NM}]$ be the Euclidean distances between the matched points. In this Project we have evaluated the following criteria to compute the matching score s between two iris images:

1. $s = NM$
2. $s = \frac{NM}{\sqrt{p_1 \times p_2}}$
3. $s = \frac{NM}{E(p_1,p_2)}$
4. $s = E(\mathbf{d})$
5. $s = max(\mathbf{d})$

with $E(.)$ representing the arithmetic mean.

A verification of the performance of our SIFT implementation for the development set is evaluated in terms of EER (%), as we vary parameters D, ε_θ and ε_ℓ. Parameter D has been varied between 0.25/255 and 3/255, whereas ε_θ and ε_ℓ have been varied between 2 and 40. The lowest EER achieved is given in Table 6.1. For comparative purposes, we also give results without trimming of false matches. We have observed during our experiments that the expansion of the input iris image (i.e. size doubling) results in worse performance, so experiments without this expansion have also be done and reported. Furthermore, DET curves for the optimal combinations given in Table 6.1 are shown in Figure 6.6.

Without trimming of false matches

		Criteria to compute the matching score				
		$s = NM$	$s = \frac{NM}{\sqrt{p_1 \times p_2}}$	$s = \frac{NM}{E(p_1,p_2)}$	$s = E(\mathbf{d})$	$s = max(\mathbf{d})$
no size doubling	**EER**	36.85 %	31.34 %	30.63 %	**20.37 %**	43.97 %
	optimal parameters	D=0.25/255	D=0.5/255	D=0.25/255	D=0.5/255	D=1.75/255
size doubling	**EER**	41.30 %	36.48 %	36.01 %	**34.52 %**	46.46 %
	optimal parameters	D=0.5/255	D=1/255	D=1/255	D=2/255	D=0.25/255

With trimming of false matches

		Criteria to compute the matching score				
		$s = NM$	$s = \frac{NM}{\sqrt{p_1 \times p_2}}$	$s = \frac{NM}{E(p_1,p_2)}$	$s = E(\mathbf{d})$	$s = max(\mathbf{d})$
no size doubling	**EER**	**9.68 %**	10.38 %	10.41 %	15.49 %	26.94 %
	optimal parameters	D=0.25/255 ε_θ=18 ε_ℓ=14	D=0.25/255 ε_θ=14 ε_ℓ=16	D=0.25/255 ε_θ=18 ε_ℓ=16	D=0.5/255 ε_θ=40 ε_ℓ=38	D=0.5/255 ε_θ=2 ε_ℓ=10
size doubling	**EER**	**15.23 %**	15.83 %	16.06 %	28.95 %	33.97 %
	optimal parameters	D=1/255 ε_θ=36 ε_ℓ=14	D=1/255 ε_θ=38 ε_ℓ=14	D=1/255 ε_θ=40 ε_ℓ=14	D=2/255 ε_θ=26 ε_ℓ=40	D=2.25/255 ε_θ=2 ε_ℓ=6

Table 6.1: Development set - SIFT matcher. Optimal combinations of the parameters D and tolerances of angle (ε_θ) and distance (ε_ℓ). Combinations resulting in the lowest EER are marked in bold.

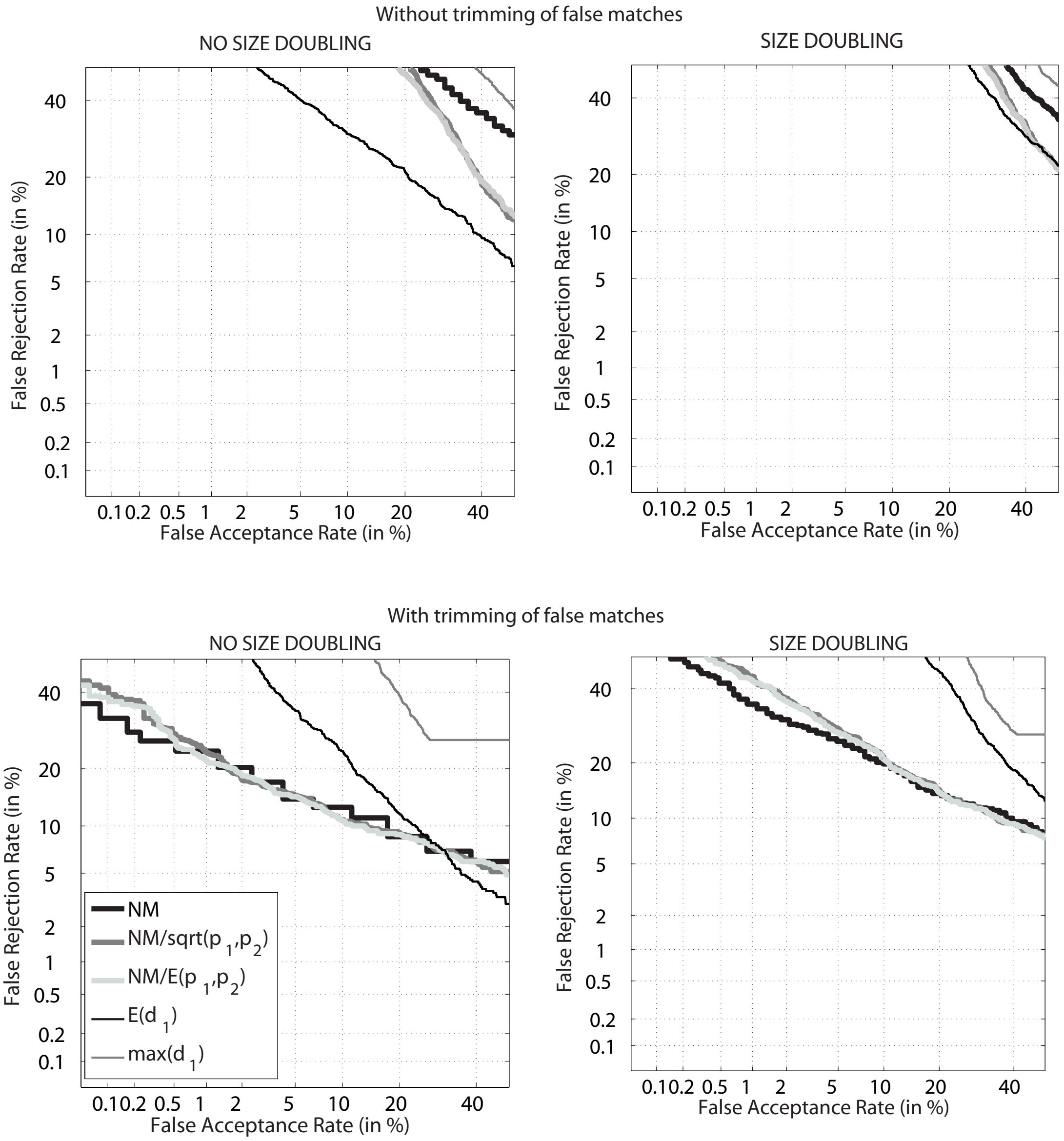


Figure 6.6: Development set - SIFT matcher. Results with the optimal combinations of the parameters D and tolerances of angle (ε_θ) and distance (ε_ℓ) given in Table 6.1.

Based on the results of Table 6.1, the best combination of parameters is D=0.25/255, ε_θ=18 and ε_ℓ=14 when using the number of matched points NM as matching score and when no image expansion is done before the Gaussian pyramid is built. We plot in Figure 6.7 the FAR-FRR curves for this combination, which allow to assess the number of matched points NM between two iris images (x-axis). We also give in Figure 6.8 the histogram of detected SIFT points in the development set of the BioSec database using the optimal value of D=0.25/255. Further analysis around this best combination is done in Figure 6.9, where we show the verification performance as we vary ε_θ and ε_ℓ when D=0.25/255 (the optimal), D=0.5/255 and D=0.75/255.

Based on the results shown in the Section, the following comments can be made:

- An initial expansion of the original image, when creating the gaussian pyramid, produces in general worst results for all the tested combinations (5 criteria to compute the score, trimming/no trimming of false matches) as shown in Table 6.1. This suggests that the size of the original images from the database (640 pixels width and 480 pixels height) is enough to obtain the required SIFT points, and the extra points obtained when doubling its size do not provide useful discriminative information. Figure 6.8 shows that the scale corresponding to the expanded image (*left plot*) results in an average of 5000-6000 detected

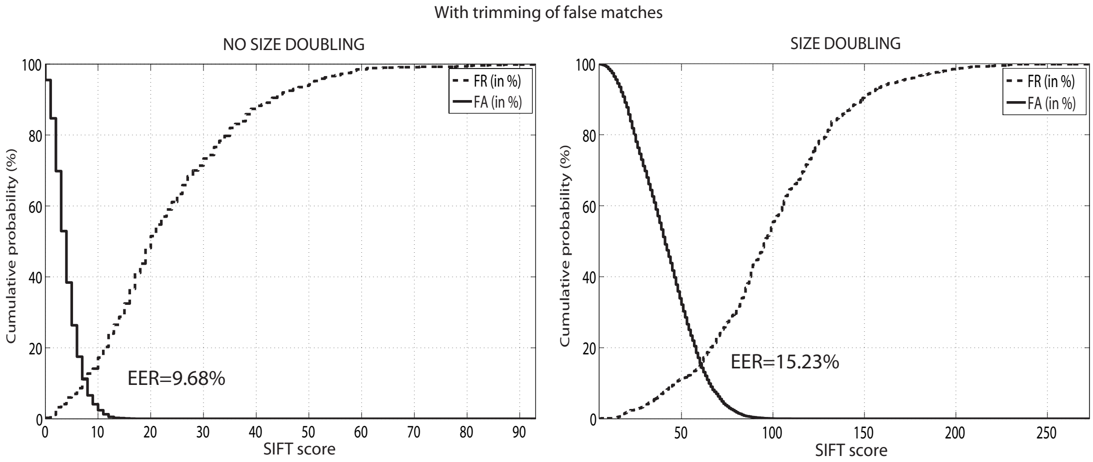


Figure 6.7: Development set - Performance of the SIFT matcher (FR=False Rejection, FA=False Acceptance). Results with the optimal combinations of the parameters D and tolerances of angle (ε_θ) and distance (ε_ℓ) for the case when the number of matched points NM is used as matching score. FA-FR curves are shown only for the case where trimming of false matches is carried out.

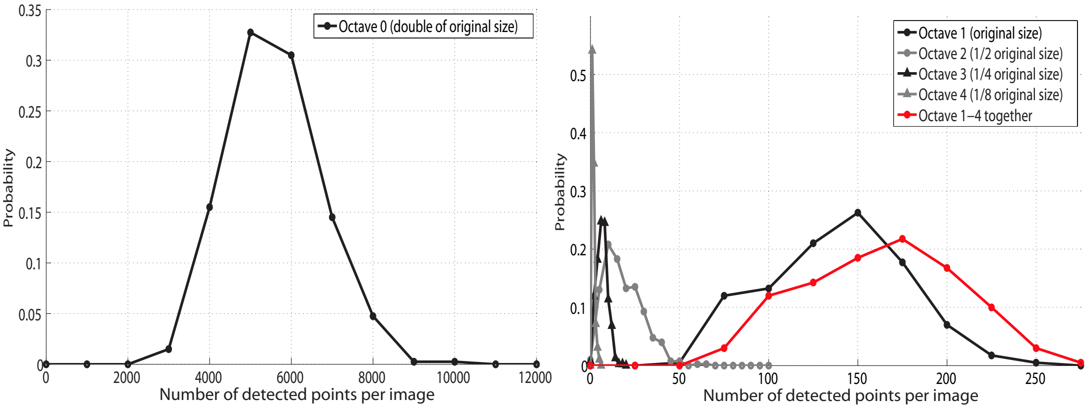


Figure 6.8: Development set - Histogram of SIFT points detected in the development set of the BioSec baseline database (parameters of the SIFT detector are σ=1.6, s=3, D=0.25/255, r=10).

points by itself in BioSec development, whereas the rest of scales together have an average of 150-175 detected SIFT points per image, more than one order of magnitude less. It should also be taken into account that these values refer only to the iris ring, which takes up a small portion of the 640×480 pixels image.

- In its paper, Lowe typically works with 2000 points in a 500×500 image (which is a similar size of the iris images of BioSec), but he refers to the whole image. As described by him, the aim of Lowe's method is to find the same object in two different images. Therefore, this approach would be able to detect whether there is a human iris in the image or not. But our goal is not that but to find out if the iris in two images belong to the same person or not. This has demanded a decrease of the thresholding value D to be able to detect enough points in the iris ring. In return, many more points than the number suggested in the original method have been detected, and therefore, when doubling the image size, the number of detected points rises too much (three times more than the number suggested by Lowe and in the smaller of the iris ring) to the point of being detrimental to the results.

- Another observation that can be made about the number of points comes from Figure 6.7, in which it can be observed that for the optimal combination (not doubling the image size), the number of matched points between two images of the same iris does not exceeds the value of 90, a little over half of the mean of the detected points per image (Figure 6.8,

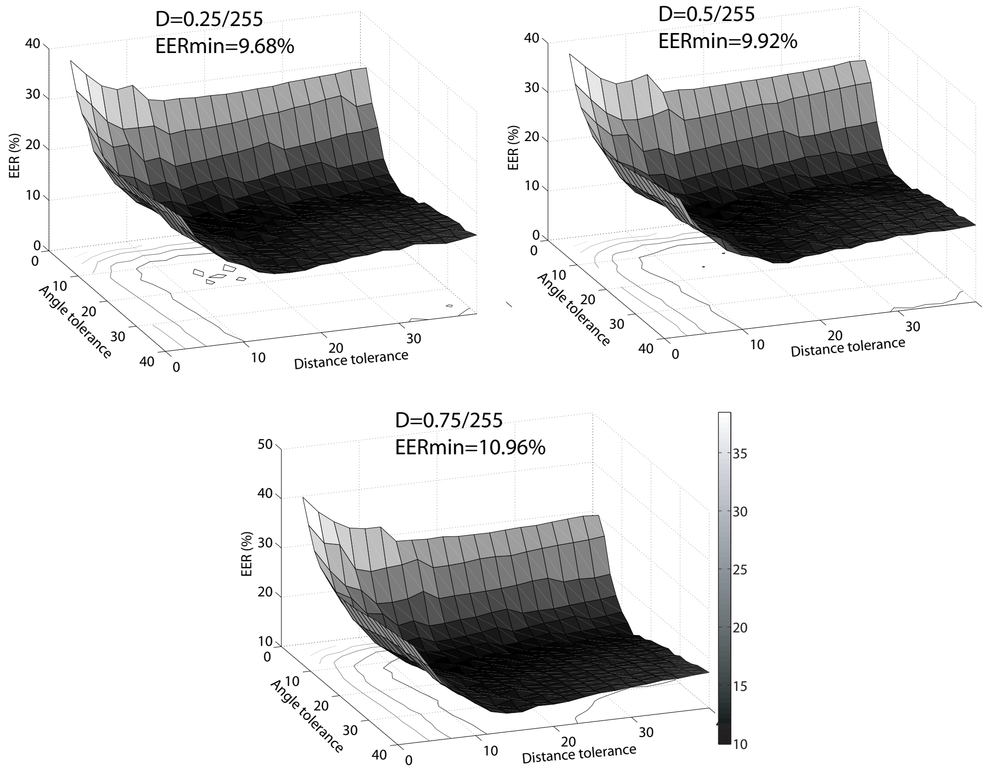


Figure 6.9: Development set - SIFT matcher. Verification results of the SIFT matcher in terms of EER (%) depending on the threshold D and the tolerances of angle (ε_θ) and distance (ε_ℓ) for the case when the number of matched points NM is used as matching score and when no image expansion is done before the Gaussian pyramid is built.

right).When doubling the image size, the maximum number of matched points rises up to around 250 (a little less than the triple), even though the number of detected points have increased almost 30 times. This validates the idea that almost all the points detected through the doubled image have no utility.

- Looking at Table 6.1, one can see that by trimming out false matches using geometric constraints, the EER is reduced considerably in all cases. Specially, for the optimum parameter combination mentioned earlier, the error rate is reduced to one fourth when introducing the trimming step (from 36.85 % to 9.68 %). Therefore, it can be concluded that an important improvement can be achieved through the system processing step, which was not included in Lowe's original implementation.

- We observe that the optimal value of D in our SIFT implementation, D=0.25/255$\simeq$0.00098, is much lower than 0.03 (as recommended in [2]). Concerning the values of the tolerances ε_θ and ε_ℓ, it can be seen in Figure 6.9 that the EER monotonically decreases as the two tolerances are increased until a minimum in the EER is reached (the exact values of ε_θ and ε_ℓ at the minimum are those indicated in Table 6.1). Once this minimum is reached, the EER is slightly increased again with the tolerances.

- For our system, the criterion used to compute the score which shows a better performance is the number NM of matched points. A possible reason for this is that the database was captured under controlled conditions and cooperative users (i.e. they were asked to look straight at the camera, keeping their eyes open and staying still during the acquisition). This is the reason why phenomena such as eyelashes/eyelids occlusion or changes in the eye gaze are not very prominent in our database. It can be seen in the DET curve for the optimum case (Figure 6.6, *bottom left*) that performing a normalization by the number of detected SIFT points on each image (p_1 and p_2) results in a similar performance, which suggests that the number of detected points between iris of the same user is indeed similar.

However, an improvement in the results is expected when using this type of normalization on non-controlled databases or those which include non-cooperative users.

- An important observation in Figure 6.6 is that for the other cases, the criteria that perform better are those which use the p_1 and p_2 values. The reason for this is that when increasing the number of detected points in an iris image, which occurs then avoiding the size doubling of the image (Figure 6.6, *bottom right*) or not doing the trimming (Figure 6.6, *top*), the possibility that the number of detected points in different images varies is increased.

- Finally, it is interesting to note that the criterion of score computation through the arithmetic mean of the Euclidean distances between the matched points ($s = E(\mathbf{d})$) gives the best performance when not applying the trimming of false matches. The reason for this may be that, when not doing trimming, the criteria that make some use of the number of matched points NM are affected by the incorrectly matched points. On the other hand, assuming that these points do not represent an important percentage of the total number of detected points, their effect in the mean of Euclidean distances seems to be less. This can be proved through the fact that when not doing trimming, the error under the criteria that make use of NM can multiply by a factor of four, whereas the error by the criterion $s = E(\mathbf{d})$ increases only by a factor of 1.3. Finally, it is important to note that the criterion $s = max(\mathbf{d})$ has always the worst performance, since it is based only on information given by a single point among all the detected ones.

6.4.2. System Evaluation

The evaluation carried out in the previous Section over the set of development data, leads to an optimal configuration of D=0.25/255, ε_θ=18 and ε_ℓ=14 for our implementation of the SIFT method, when using the number of matched points NM as matching score and when no image expansion is done before the Gaussian pyramid is built.

To validate the conducted development and optimization processes, a system performance is shown next. To do so, the optimum configuration as explained before has been used. The experiments have been carried out over the 150 users of the *test set* from BioSec, which have not been used in any previous adjustment.Besides, the performance of the reference system will also be shown to allow a comparison between both systems, as well as the performance of a combination of both systems.

Figure 6.10 comparatively shows the performance of the two matchers using DET curves, both on the development and on the test set of the BioSec database. For the fusion of the SIFT and baseline matchers, we use the sum rule with tanh normalization [93]:

$$s' = \frac{1}{2}\left\{\tanh\left(0{,}01\left(\frac{s-\mu_s}{\sigma_s}\right)\right)+1\right\} \tag{6.1}$$

where s is the raw similarity score, s' denotes the normalized similarity score, and μ_s and σ_s are respectively the estimated mean and standard deviation of the genuine score distribution. Prior to the fusion, scores of both systems are normalized using the mentioned tanh operator to be in the same comparative range. As stated before, normalization parameters of the two matchers are computed using scores from the *development set* only.

Thus, it can be seen that the performance of the SIFT system for the evaluation data is similar to that obtained for the development data only slightly worst.On the other hand, the reference system shows a better performance that the SIFT system, with less than half error rates. Experimental studies have suggested that the use of Gabor filters and their derivatives show the best performance for iris systems up to date [9]. However, the promising results of the developed system open allow to think of its utility as an effective iris recognition method. The effectiveness of the SIFT method also becomes apparent when observing the improvement that

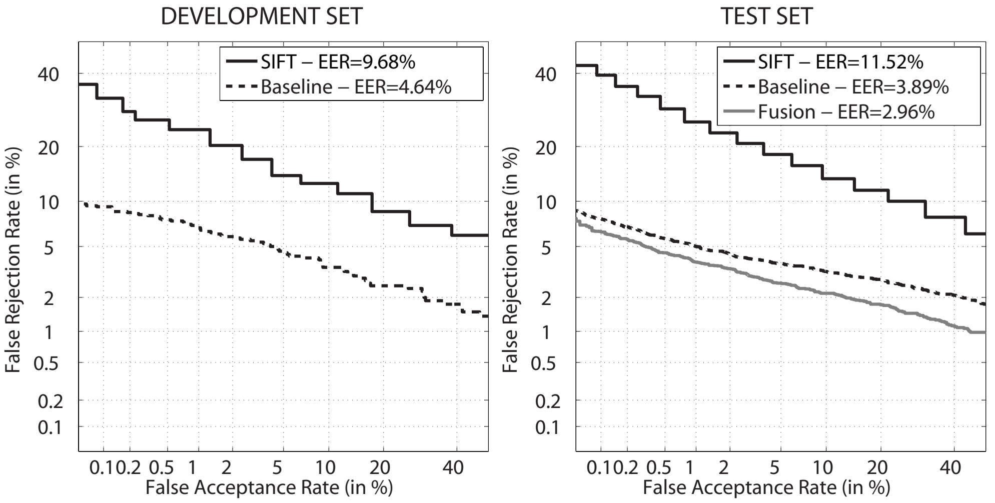


Figure 6.10: Performance of the SIFT and the baseline matchers and their fusion results.

takes place when merging both systems together, obtaining an EER of 2.96 % versus the 3.89 % of the reference system. Although the performance of our implementation is below popular matching approaches based on transformation to polar coordinates and Log-Gabor wavelets, their fusion provides a performance improvement of 24 % in the EER. This is because the sources of information used in the two matchers are different, providing complementary sources of information.

6.4.3. System Attacks

As mentioned in Chapter 3, despite their advantages, biometric systems have some drawbacks, among which we have its vulnerability to to external attacks which could decrease its level of security. Part of the work carried out during this Project has focused on the analysis of vulnerabilities of iris systems to attacks. We have concentrated our efforts in studying direct attacks on iris-based verification systems. Here, the sensor is attacked using synthetic biometric samples. For this purpose we have built a database with synthetic iris images generated from the 50 users of the BioSec *development set*. It is worth noting that, in this type of attacks, no specific knowledge about the system is needed. Furthermore, the attack is carried out in the analog domain, outside the digital limits of the system, so digital protection mechanisms (digital signature, watermarking, etc) cannot be used. A reduced version of this study applied only to the baseline matcher, was published by the author in [14].

Fake Iris Database

A new iris database has been created in this Project using iris images from the 50 users of the BioSec *development set*. The process is divided into three steps: *i*) first original images are preprocessed for a better afterwards quality, then *ii*) they are printed on a piece of paper using a commercial printer as shown in Figure 6.11 (*left*), and lastly, *iii*) printed images are presented at the iris sensor, as can be seen in Figure 6.11 (*right*), obtaining the fake image. The fake iris database follows the same structure of the original BioSec *development set*. Therefore, data for the experiments consists of 50 users × 2 eyes × 4 images × 2 sessions = 800 fake iris images, and its corresponding real images. Acquisition of fake images has been carried out with the same iris camera used in BioSec, a LG IrisAccess EOU3000.

To correctly create a new database, it is necessary to take into account factors affecting the quality of acquired fake images. The main variables with significant importance for iris quality are found to be: preprocessing of original images, printer type and paper type. We tested two

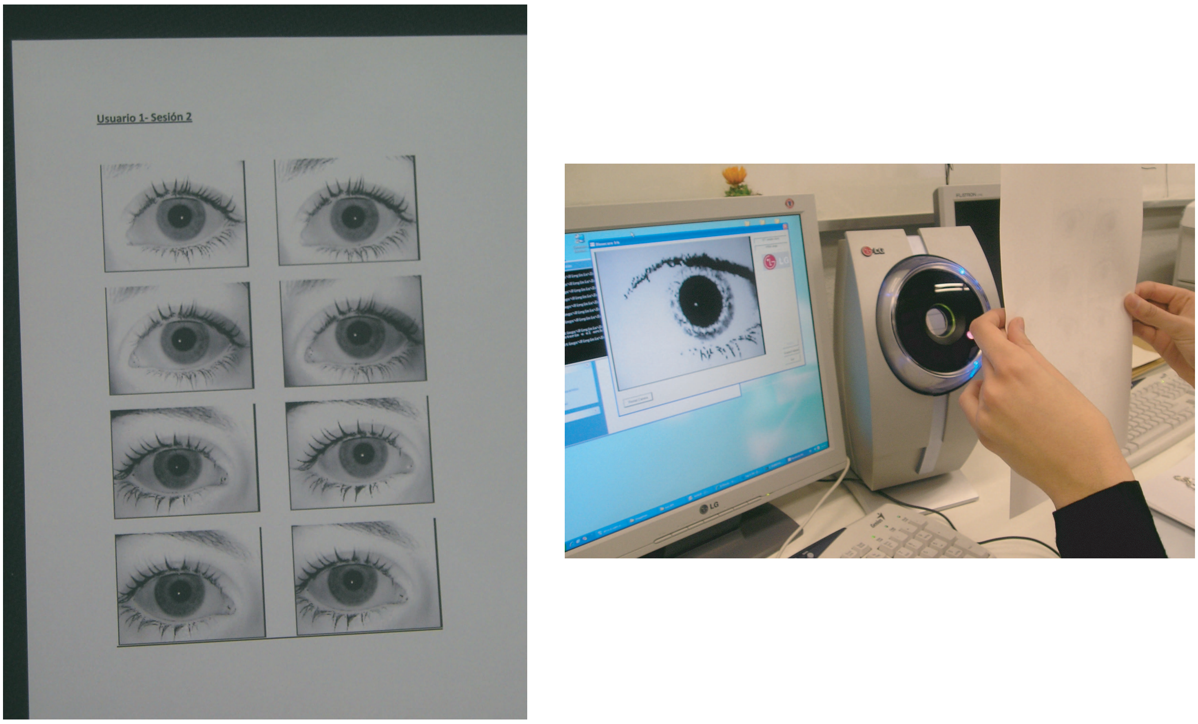


Figure 6.11: Iris capture preparation.

PRINTER	PAPER	PREPROCESSING [?]
Ink Jet Laser	White paper Recycled paper Photographic paper High resolution paper Butter paper Cardboard	Histogram equalization Noise filtering Open/close Top hat

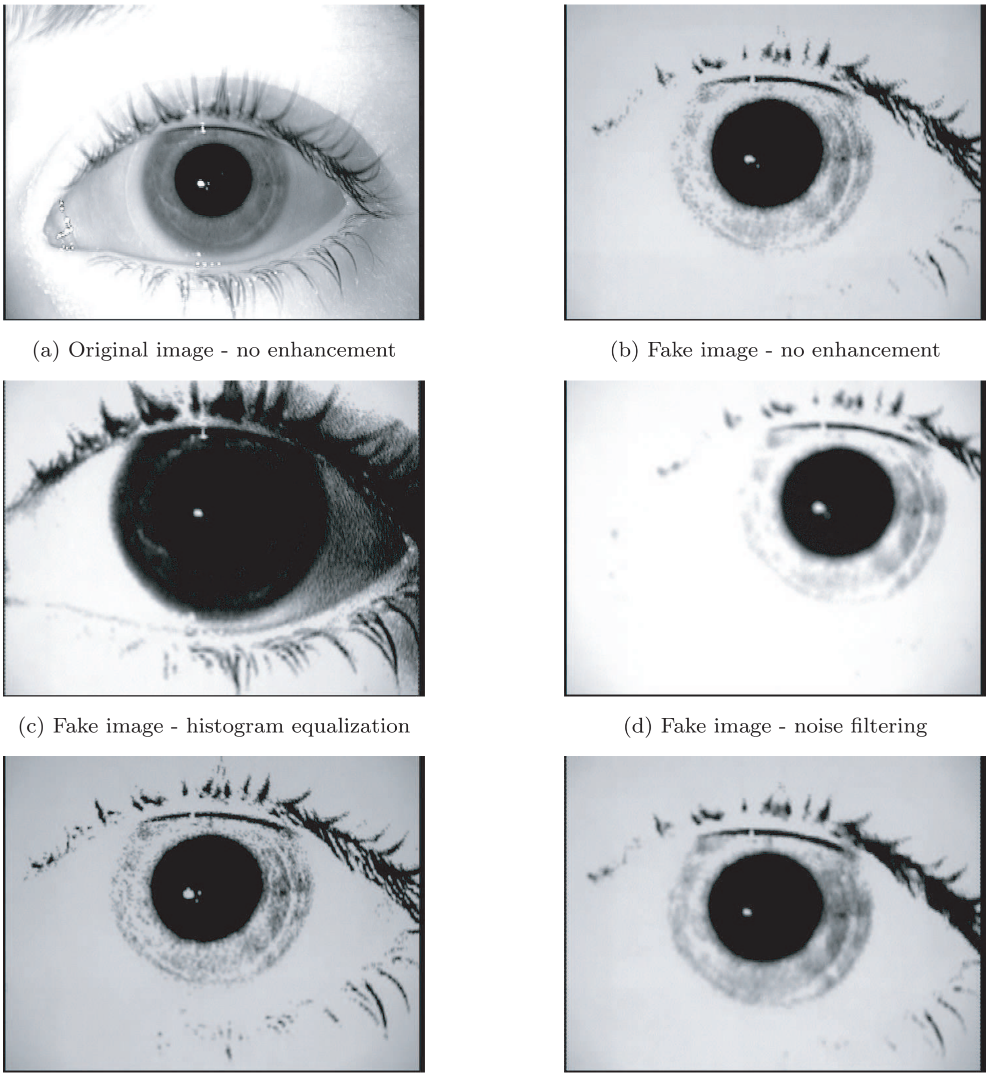
Table 6.2: Options tested for fake iris generation.

different printers: a HP Deskjet 970cxi (inkjet printer) and a HP LaserJet 4200L (laser printer). They both give fairly good quality. On the other hand, we observed that the quality of acquired fake images depends on the type of paper used. Here comes the biggest range of options. All the tested types appear in Table 6.2. In our experiments, the preprocessing is specially important since it has been observed that the iris camera does not capture original images printed without previous modifications. Therefore we have tested different enhancement methods before printing in order to acquire good quality fake images. The options tested are also summarized in Table 6.2. By analyzing all the possibilities with a small set of images, the combination that gives the best segmentation results and therefore the best quality for the afterwards comparison has been found to be the inkjet printer, with high resolution paper and an Open-TopHat preprocessing step. In Figure 6.12, examples using different preprocessing techniques with this kind of paper and inkjet printer are shown. Some examples of the fake images acquired with the final chosen configuration are shown in Figure 6.13

Attacks Protocol

For the experiments, each eye in the database is considered as a different user. In this way, we have two sessions with 4 images each for 100 users (50 donors × 2 eyes per donor).

Two different attack scenarios are considered in the experiments and compared to the system normal operation mode:



(a) Original image - no enhancement

(b) Fake image - no enhancement

(c) Fake image - histogram equalization

(d) Fake image - noise filtering

(e) Fake image - TopHat

(f) Fake image - Open+TopHat

Figure 6.12: Acquired fake images with different modifications using high quality paper and inkjet printer.

- **Normal Operation Mode (NOM)**: both the enrollment and the test are carried out with a real iris. This is used as the reference scenario. In this context the FAR (False Acceptance Rate) of the system is defined as the number of times an impostor using his own iris gains access to the system as a genuine user, which can be understood as the robustness of the system against a zero-effort attack. The same way, the FRR (False Rejection Rate) denotes the number of times a genuine user is rejected by the system.
- **Attack 1**: both the enrollment and the test are carried out with a fake iris. In this case the attacker enrolls to the system with the fake iris of a genuine user and then tries to access the application also with a fake iris of the same user. In this scenario an attack is unsuccessful (i.e. the system repels the attack) when the impostor is not able to access the system using the fake iris. Thus, the attack success rate (SR) in this scenario can be computed as: SR = 1 − FRR.
- **Attack 2**: the enrollment is performed using a real iris, and tests are carried out with fake iris. In this case the genuine user enrolls with his/her iris and the attacker tries to access the application with the fake iris of the legal user. A successful attack is accomplished when the system confuses a fake iris with its corresponding genuine iris, i.e., SR = FAR.

In order to compute the performance of the system in the normal operation mode, we follow

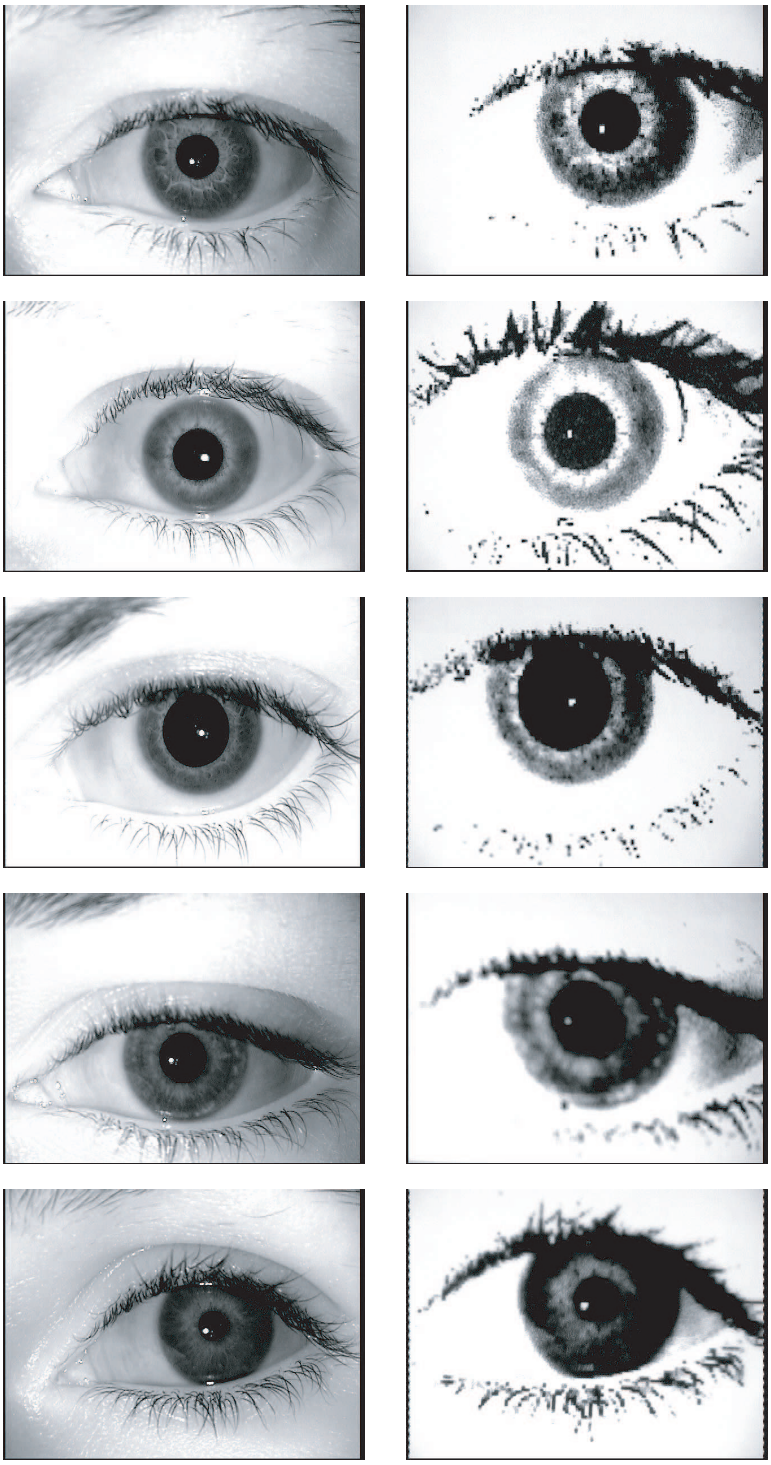
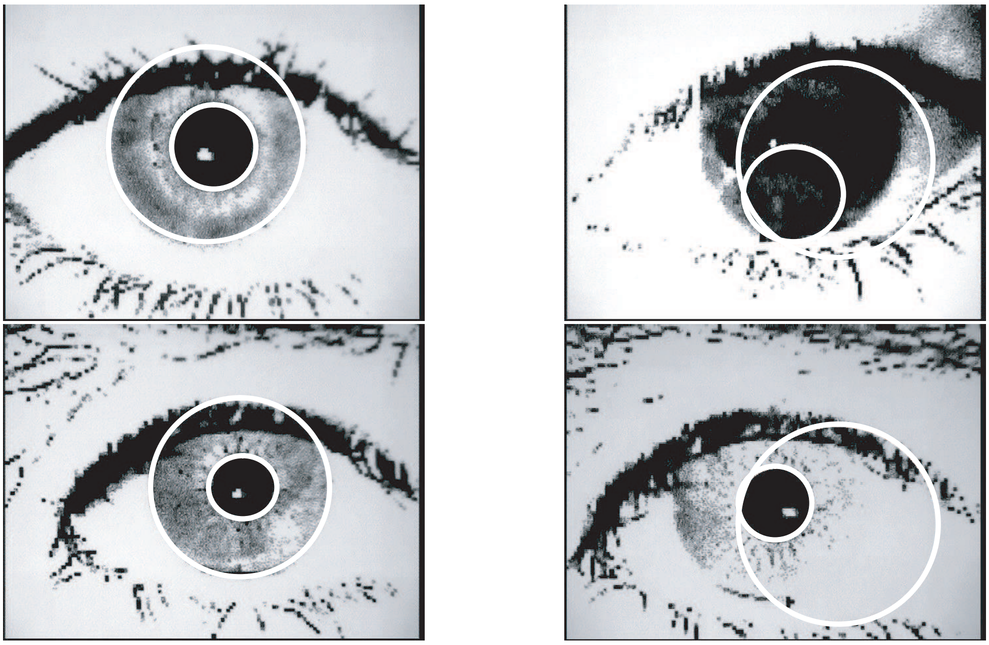


Figure 6.13: Real iris from BioSec baseline database (*left*) and their corresponding synthetic "fake" images (*right*) acquired with the optimum configuration.

the experimental protocol of Section 6.1. Similarly, to compute the FRR in attack 1, all the fake images of the first session of each user are compared with the corresponding fake images of the second session. In the attack 2 scenario, only the impostor scores are computed matching all the 4 original samples of each user with its 4 fake samples of the second session.

Results

For the attack experiments, the segmentation procedure follows the description of that explained in Sec. 6.2. However, for a more realistic scenario, the previous inspection and manual correction used during the SIFT system optimization will be avoided. Therefore, the only used segmented data will be that obtained through an automatic computation. As a result, not all the images are segmented successfully, so it was not possible to use all the eye images for testing experiments. The number of correctly segmented images are 792 for the original database (99 % of the 800 available) and 574 for the fake database (71.75 % of the 800). In Figure 6.14, several examples of fake images with correct and incorrect iris detection are plotted. It is worth noting than more than 70 % of fake images pass through the segmentation and normalization stages, and they are input into the feature extraction and matching stages.



(a) Correct iris detection

(b) Incorrect iris detection

Figure 6.14: Examples of fake images with correct iris detection (left) and incorrect iris detection (right).

For the SIFT matcher, several experiments have been performed, following three of the criteria proposed for the computation of the matching score (using the optimal configurations shown in Table 6.1 with no size doubling and with trimming of false matches). We plot in Figure 6.15 the cumulative distribution function of the SIFT matching scores corresponding to the two attacks when the number of matched points NM is used as matching score (this allow to assess the number of matched points NM between two iris images for the two attacks, see x-axes). We also give in Figure 6.16 the histogram of detected SIFT points in the fake database.

In Table 6.3 we show the Success Rate (SR) of the direct attacks against the baseline and the SIFT matchers at four different operating points, considering only the matchings between correctly segmented images. The decision threshold is fixed to reach a FAR={0.1, 1, 2, 5} % in the normal operation mode (NOM), and then the success rate of the two proposed attacks is computed. The working points in the normal operation mode (NOM) correspond to the DET curves in Figures 6.6 (*bottom, left*) for the SIFT matcher, and 6.10 (*left*) for the baseline matcher.

It is important to notice the high vulnerability of the baseline matcher compared to the developed SIFT matcher. We observe that in all the operating points, the baseline matcher is vulnerable to the two attacks (i.e. a success rate of about 20 % or higher is observed). This is specially evident as the FAR in the normal operation mode is increased, being successful in about 35 % of the attack 1. The noticeable difference between both systems can be explained by their operation. The SIFT matcher is based on the detection of characteristic points that fulfill certain local criteria, such as: being a local extrema, not having low contrast, not being situated along an edge, etc. The baseline matcher, on the other hand, is based on filtering and codifying the whole iris region. In this sense, an important variation of the properties of the captured image

BASELINE MATCHER

NOM	**Attack 1**	**Attack 2**
FAR - FRR (%)	SR (%)	SR (%)
0.1 - 9.25	19.81	19.33
1 - 6.75	26.81	23.78
2 - 5.88	29.14	25.66
5 - 4.56	34.15	28.99

SIFT MATCHER - MATCHING SCORE NM

NOM	**Attack 1**	**Attack 2**
FAR - FRR (%)	SR (%)	SR (%)
0.1 - 30.63	3.26	0.09
1 - 22.13	7.69	0.43
2 - 18.75	9.32	0.94
5 - 13.44	15.15	2.74

SIFT MATCHER - MATCHING SCORE $s = \frac{NM}{\sqrt{p_1 \times p_2}}$

NOM	**Attack 1**	**Attack 2**
FAR - FRR (%)	SR (%)	SR (%)
0.1 - 41.19	1.28	0.94
1 - 23.81	3.73	2.4
2 - 17.81	5.48	3.42
5 - 14.69	8.28	5.05

SIFT MATCHER - MATCHING SCORE $s = \frac{NM}{E(p_1,p_2)}$

NOM	**Attack 1**	**Attack 2**
FAR - FRR (%)	SR (%)	SR (%)
0.1 - 38.5	0.93	0.26
1 - 21.63	3.61	1.45
2 - 18.63	4.43	1.88
5 - 14.5	7.93	3.94

Table 6.3: Evaluation of the baseline and the SIFT matchers to direct attacks. NOM refers to the system normal operation mode and SR to the success rate of the attack.

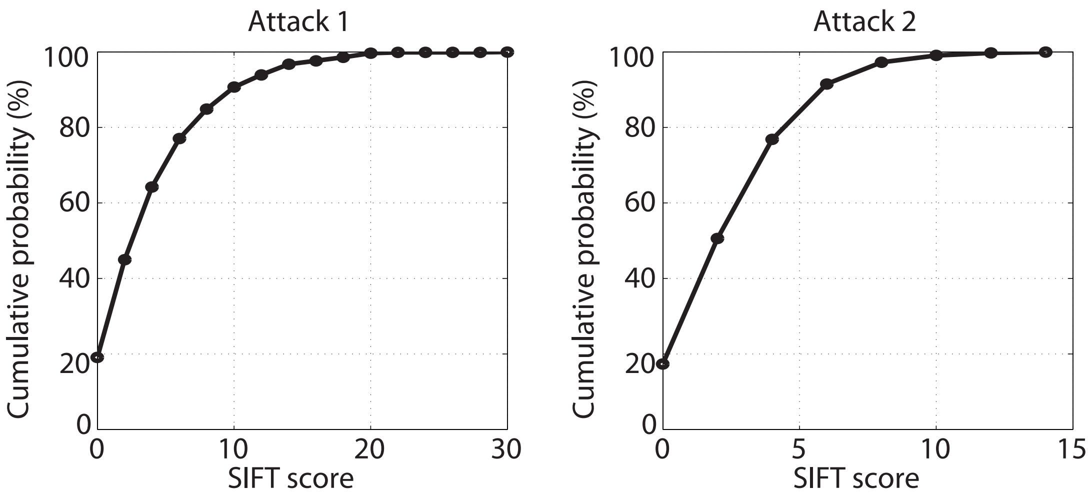


Figure 6.15: System attacks - Cumulative distribution function of the SIFT matching scores corresponding to the two attacks. Results are shown for the case when the number of matched points NM is used as matching score.

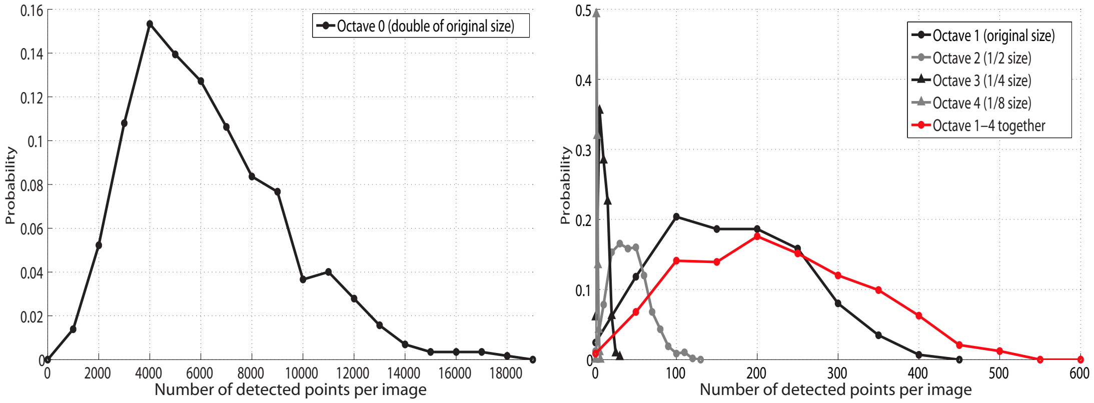


Figure 6.16: Fake database - Histogram of SIFT points detected (parameters of the SIFT detector are σ=1.6, s=3, D=0.25/255, r=10).

(as the one experienced by a fake image), has a greater impact in the detection of local features than in a filtering of the whole iris texture, which has an "averaging" effect with the neighboring regions. This effect can also be observed in other biometric traits such as fingerprint, where the recognizers based on the detection of local characteristic points of the fingerprint are much more sensible to the variation of the properties of the image, whereas the recognizers based on texture filtering show a smaller sensibility due to the previously mentioned "averaging" [17].

On the same thinking path, we can observe that the distribution of the number of detected points in the fake images is considerably different from that of the original database. By comparing the red curves in Figures 6.16 and 6.8, we observe that the distribution of the fake database expands from zero to 550, a much greater range than the one of the real image database (50-275). The fact that the fake distribution expands to zero suggest that for certain images, non of the criteria required for the SIFT detector are fulfilled, resulting in very little number of points detected. However, a greater expansion of the distribution than the original in the direction of greater values suggests that in some images there is a large number of spurious SIFT points which cannot be found in the real iris image. In any case, we can observe that the number of matched points between images for both attacks is very low, see Figure 6.15, which explains its low vulnerability (less than 20 matched points for attack 1 and less than 10 points for attack 2). In contrast, when matching genuine iris images (see Figure 6.7, *left*), the number of matched points rises up to 70-80. This allows to conclude that the recognition based on SIFT points detection is quite robust to the direct attacks evaluated here.

It is also remarkable the high success rates observed for attack 1 with the baseline matcher, which are quite similar to attack 2. In the attack 1, an intruder would be correctly enrolled in the system using a fake image of another person and at a later date, he/she would be granted access to the system also using a fake image. The success rates for the attack 1 with the SIFT matcher is consistently smaller for the whole operational range, reaching success rates of only about 8-9 % for high FAR (15 % in the worst case).

7
Conclusions and Future Work

The present Project contains two interconnected lines of investigation. A SIFT iris oriented recognition system has been studied, developed, implemented and evaluated following the actual state of the art. Along with this work, a study of the vulnerabilities of iris recognition biometric systems, more specifically to direct attacks, has been presented, providing another element to asses the system performance.

The importance of proposed SIFT system relies on the fact that traditional iris recognition systems, based on accurate segmentation and transformation to polar coordinates, rely on cooperative data, where the irises have centered gaze, little eyelashes or eyelids occlusion, and illumination is fairly constant [8]. The SIFT-based method does not require polar transformation or highly accurate segmentation, and it is invariant to illumination, scale, rotation and affine transformations [2]. This makes the SIFT approach feasible for biometric recognition of distant and moving people, e.g. the "Iris on the Move" project [28], where a person is recognized while walking at normal speed through an access control point such as those common at airports. Currently this is one of the research hottest topics within the international biometric community [94], which drastically reduces the need of user's cooperation, and it will be an important source of future work.

To investigate this new biometric trend, a SIFT system has been implemented in this Project following [2]. However, this system was focused on the search of an specific object in two different images. Since our goal is personal identification through iris recognition, the original system, which is characterized by a number of parameters, has been adjusted to fulfill our requirements.

One of the optimizations focuses on the D parameter of the SIFT algorithm, which in our implementation is much lower (D=0.25/255≃0.00098) than the one recommended in [2] (D=0.03). The reason for this adjustment derives from the use we want to make of the SIFT system: out of all the detected points, only those in the iris ring region will be valid for matching. For a reliable identification, a minimum number of these points is required. If this number is too small, only the existence of an iris could be assumed, but no identity could be claimed. By lowering the threshold D, more characteristic points to define the iris region were detected.

Among this study, different matching score criteria have also been tested. In a recognition system, a correct matching is as important as a correct feature extraction process. Between the five evaluated criteria, the number of matched points, NM shows the best performance. However, it should be noticed that these tests were carried out over a well controlled acquired database. This means that images from the same iris are generally very similar, and therefore, the number of extracted SIFT points is similar too. For a non-controlled databases or those which include non-cooperative users is expected that other criterion, such as the mean of Euclidean distances between matched points, will prove better results.

Another of the modifications performed on Lowe's system [2] focuses on the Gaussian pyramid. A significant increase on the number of detected SIFT points in the zero scale (belonging to the doubled size original image) respect to the original system, led to the study of the system performance without the doubling step. Through experimental results we have proven that doubling the image size during this step is detrimental to the matching score. This suggests that the original image size of our database is enough for a correct matching, and the increase in characteristic points in the scale zero of the Gaussian pyramid produces no discriminant information.

Thanks to a deep study and comprehension of the SIFT method, it has been possible to propose some improvements to the original system. On of them is the trimming of false matches based on geometric limitations. This addition to the method is derived from the fact that if the same iris appears in two different images, when placed side by side and draw matching lines, true matches must appear as parallel lines with similar lengths. In this Project it is shown the important improvement can be achieved through the system processing step, which was not included in Lowe's original implementation [2].

On top of presenting a comparison between SIFT methods, the work in this Project aims to prove the effectiveness of the system related to existing iris recognition methodologies. After the studies that have been carried out, we can conclude that traditional systems based on Gabor filters show the best performance up to date. However, the promising results of the developed system open allow to think of its utility as an effective iris recognition method, specially when observing the improvement that takes place when merging both systems together. Future work concerning the development of the SIFT matcher will be focused on the detection of eyelids, eyelashes and specular reflections [9], thus discarding SIFT keypoints computed in these regions. We are also working on the inclusion of local iris quality measures [86] to account for the reliability of extracted SIFT points, so if the quality is high for two matched points, they will contribute more to the computation of the matching score.

The availability of an Open Source system such as the one implemented gives many opportunities of improvement. Just as we have done for iris recognition, SIFT systems have proven to be reliable for other biometric recognition areas, after a consistent adjustment. Therefore we are quite satisfied with the work carried out for this Project in this area.

As for the effects of system attacks, an evaluation of the vulnerabilities to direct attacks of iris-based verification systems has been presented. The attacks have been evaluated using fake iris images created from real iris of the BioSec baseline database. We printed iris images with a commercial printer and then, we presented the images to the iris sensor. Different factors affecting the quality of acquired fake images have been studied, including preprocessing of original images, printer type and paper type. We have chosen the combination giving the best quality and then, we have built a database of fake images from 54 eyes, with 8 iris images per eye. Acquisition of fake images has been carried out with the same iris camera used in BioSec.

Two attack scenarios have been compared to the normal operation mode of the system using a publicly available iris recognition system. The first attack scenario considers enrolling to the system and accessing it with fake iris. The second one represents accessing a genuine account with fake iris. To simulate a more realistic situation, only data obtained through automatic computation will be used. However, the *Success Rate* (SR) of the attacks is evaluated only over the correctly segmented images (99 % of the images in the original database were correctly segmented and over a 71 % for the fake iris database).

The obtained results are very remarkable. Experiments showed that the baseline system is highly vulnerable to the two evaluated attacks in all the operating points. However, the performance of the implemented SIFT system to direct attacks proved to be better than the baseline for all the tested score matchers. The reason for this is its greater sensibility to the variation of the properties in the captured image. It is also noticeable that the SR of the baseline system for both attacks is very similar for this system, whereas the SR observed for attack 1 with the SIFT matcher is consistently smaller than for attack 2. Liveness detection procedures are possible countermeasures against direct attacks. For the case of iris recognition systems, light reflections or behavioral features like eye movement, pupil response to a sudden lighting event, etc. have been proposed [81, 82]. This research direction is another source of future work.

Parallel to the work presented in this Project, a quality measures study of the captured images in iris biometric systems has been started. Together with this, the goal of the author is to acquire a deep understanding of iris recognition systems, in order to develop a reliable identification method, that includes different characteristics and scenarios.

8

Conclusiones y trabajo futuro

El presente Proyecto consta de dos líneas de investigación interrelacionadas. En primer lugar, se ha estudiado, desarrollado, implementado y evaluado un sistema de reconocimiento biométrico basado en las características SIFT, según el estado actual del arte. Al mismo tiempo, se ha llevado a cabo un estudio de las vulnerabilidades de los sistemas biométricos basados en iris, específicamente, ante ataques directos, lo que dota al sistema de una forma más de evaluación.

La importancia del sistema SIFT propuesto radica en el hecho de que los sistemas tradicionales de reconocimiento de iris, basados en una segmentación precisa y una transformación a coordenadas polares, asumen una colaboración por parte del usuario a la hora de adquirir las muestras. Esto significa que para un correcto funcionamiento del sistema, los iris capturados deben tener la mirada centrada, una iluminación más o menos constante, y poca intrusión por parte de los párpados y pestañas [8]. El método presentado, basado en características SIFT, no requiere una transformación a coordenadas polares ni gran precisión durante la fase de segmentación. Además, una de sus principales cualidades es su invariancia al escalado, la rotación, transformaciones lineales y ligeros cambios de iluminación [2]. Todo esto hace que la aproximación SIFT sea muy conveniente en reconocimiento biométrico a distancia y con personas en movimiento, como por ejemplo el proyecto "Iris on the Move" [28], donde una persona es reconocida mientras camina a velocidad normal a través de un punto de control de acceso, como por ejemplo los encontrados en los aeropuertos. Actualmente este es uno de los temas en auge entre la comunidad internacional de biometría [94], puesto que reduce de forma drástica la necesidad de cooperación por parte del usuario. Por ello, ésta será una de las vías más importantes de trabajo futuro.

Acorde con dicha nueva tendencia de la biometría, en este Proyecto se implementa un sistema SIFT siguiendo el modelo presentado en [2]. Sin embargo, este método fue diseñado para localizar un objeto en dos imágenes diferentes. Puesto que nuestro objetivo es el reconocimiento de personas basado en el análisis del iris, el sistema original, el cual está caracterizado por una serie de parámetros, ha sido modificado para acomodarse a nuevos requisitos. Una de las optimizaciones realizadas se centra en el parámetro D del algoritmo SIFT, el cual tiene un valor mucho menor para nuestra implementación (D=0.25/255$\simeq$0.00098) que el propuesto en [2] (D=0.03). Esto se debe al uso que estamos haciendo del método SIFT: de todos los puntos detectados en la imagen sólo nos servirán aquellos que se encuentren dentro del anillo del iris. Para realizar una comparación fiable, es necesario tener un mínimo número de puntos característicos en esta zona, ya que si dicho número no fuese suficiente, sólo se podría detectar la existencia o no de un iris, pero no distinguir su identidad. Por ello, el umbral D se ha reducido para aceptar más puntos, logrando así caracterizar la región del iris.

Dentro de estas pruebas se han incluido además distintos criterios para el cómputo del matching score entre dos imágenes. En un sistema de reconocimiento, la importancia de un buen matching está a la altura de una correcta extracción de características. De los cinco criterios usados, el que mejor resultados obtiene para nuestra base de datos es el de número de matched points NM. Sin embargo, es importante señalar que dicha base de datos ha sido adquirida en un entorno controlado, con situaciones muy similares en todas las capturas, por lo que el número de puntos SIFT extraídos en dos imágenes del mismo usuario es muy parecido. Es probable que una mayor variabilidad de dicho entorno hiciese que el criterio NM no fuese el óptimo. Así, por ejemplo, sin el post-procesado de falsos matching, el criterio que muestra un mejor rendimiento del sistema es el de la media de distancias Euclídeas entre puntos identificados.

Otra de las modificaciones realizadas sobre el sistema de Lowe [2] se centra en la creación de la pirámide gaussiana. Un aumento muy significativo respecto al sistema original de la detección de puntos SIFT, sobre la escala cero (perteneciente a la imagen a analizar con tamaño doble), motivó el estudio del rendimiento del sistema sin dicha escala de duplicación. A través de resultados experimentales hemos demostrado que un aumento del tamaño inicial de la imagen de análisis no mejora el matching score. Ello sugiere que el tamaño de las imágenes originales es suficiente para obtener el mínimo número de puntos SIFT requerido para un correcto matching, por lo que un mayor número de puntos no produce información discriminante.

Gracias a un estudio detallado y comprometido del método SIFT, ha sido posible proponer ciertas mejoras sobre el sistema original. Una de ellas es el trimming de falsos matching basado en limitaciones geométricas. El razonamiento detrás de esta decisión es simple: si un mismo iris aparece en dos imágenes distintas, al compararlas, la correspondencia entre puntos característicos debe mostrar cierto paralelismo y la distancia entre puntos debe ser más o menos equivalente. En este Proyecto se demuestra la gran mejora en resultados obtenida al incluir este post-procesado a la implementación de Lowe [2].

Además de realizar una comparación con los sistemas de SIFT existentes, en este Proyecto se pretende demostrar la efectividad de este sistema respecto a las distintas metodologías de reconocimiento de iris. Tras los estudios realizados, podemos concluir que los sistemas tradicionales basados en filtros de Gabor siguen obteniendo mejores resultados que el sistema desarrollado. Sin embargo, la efectividad del nuevo sistema es prometedora, especialmente tras observar una mejora de resultados al fusionar el sistema tradicional con el SIFT. El trabajo futuro concerniente al desarrollo del matcher SIFT se centra en la detección de pestañas, párpados y reflejos especulares [9], lo que permitirá desechar puntos SIFT detectados en estas zonas. También estamos trabajando en la inclusión de medidas locales de calidad de iris [86], a partir de las cuales se podría tener en cuenta la fiabilidad de los puntos SIFT extraídos, de forma que si la calidad de un punto es alta, eéste contribuya con mayor peso al cálculo del matching score.

La disponibilidad de un sistema de código abierto de este tipo abre las puertas a muchas oportunidades de mejora e investigación. Por ejemplo, siguiendo las pautas recogidas en este Proyecto, el sistema implementado se puede adaptar a las necesidades de otros sistemas de reconocimiento biométrico como, por ejemplo, cara o huella. Es por que nos encontramos satisfechos del trabajo realizado en este area.

En cuanto a los efectos de los ataques a los sistemas, en este Proyecto se presenta una evaluación de las vulnerabilidades ante ataques directos de los sistemas de reconocimiento basados en iris. Los ataques han sido evaluados usando imágenes de iris falsas creadas a partir de iris reales de la base de datos BioSec baseline. Las imágenes de iris han sido impresas con una impresora comercial y después presentadas al sensor de iris. Diferentes factores referentes a la calidad de las imágenes falsas adquiridas han sido estudiados, incluyendo en ellos el pre-procesado de las imágenes originales, el tipo de impresora y el tipo del papel. Tras elegir la combinación de dichos factores que resulta en una mejor cualidad, hemos construido una base de datos falsa, la cual contiene 54 ojos, con 8 imágenes de iris por ojo. La adquisición de imágenes falsas se ha llevado a cabo con la misma cámara de iris usada en BioSec.

Se han creado dos escenarios de ataque diferentes, los cuales han sido comparados con el modo de operación normal del sistema, usando un sistema de reconocimiento de iris disponible públicamente. El primer escenario de ataque consiste en registrarse en el sistema y acceder al mismo, usando en ambos casos un iris falso. El segundo representa el intento de acceso a una cuenta original usando un iris falso. Para simular una situación más realista, durante estos experimentos sólo se ha utilizado la información obtenida a través de cómputos automáticos. Sin embargo, la *Tasa de acierto* de los ataques fue calculada únicamente sobre las imágenes correctamente segmentadas (99 % de las imágenes de la base de datos original fueron correctamente segmentadas y más del 71 % de las de la base de datos falsa).

Los resultados obtenidos en esta sección son de especial relevancia. A través de experimentos hemos demostrado que el sistema tradicional es altamente vulnerable a ambos ataques, en cualquier punto de operación. Sin embargo, el sistema SIFT demostró un comportamiento mucho más robusto ante dichos ataques con cualquiera de los score matchers. La justificación para dicho comportamiento es su mayor sensibilidad a la variación de las propiedades de la imagen capturada. También es notable observar que, para el sistema tradicional, la tasa de éxito de ambos ataques es muy similar, mientras que en el matcher SIFT, el éxito del ataque 1 es siempre inferior que en el ataque 2. Medidas de detección de vida son las soluciones más barajadas ante posibles ataques directos. Para el caso de sistemas basados en reconocimiento de iris, reflejos de luz o características de comportamiento como el movimiento del ojo o la respuesta de la pupila ante una luz repentina, han sido propuestos en [81, 82]. Esta es otra de las direcciones de nuestro trabajo futuro.

De forma paralela al trabajo presentado en este Proyecto, se ha comenzado también con un estudio de medidas de calidad de imágenes capturadas por sistemas biométricos de iris. A través de todo ello, la autora busca un conocimiento más completo del funcionamiento de los sistemas de reconocimiento basados en iris, para lograr desarrollar un método de identificación fiable y eficaz que tenga en cuenta las distintas posibilidades de características y escenarios.

Glosario de acrónimos

Glosario

- **AES**: Advanced Encryption Standard
- **DCT**: Discrete Cosine Transform
- **DET**: Detection Error Tradeoff
- **DNA**: Deoxyribonucleic acid
- **DTW**: Dynamic Time Warping
- **EER**: Equal Error Rate
- **FAR**: False Acceptance Rate
- **FFT**: Fast Fourier Transform
- **FRR**: False Rejection Rate
- **GLCM**: Gray Level Co-ocurrence Matrix
- **HD**: Hamming Distance
- **HMM**: Hidden Markov Models
- **IS**: Iris signature
- **SIFT**: Shift Invariant Feature Transform
- **SR**: Success Rate
- **WED**: Weighted Euclidean Distance

Las siguientes *abreviaciones* han sido usadas: Chap. (chapter), Sec. (section), Fig. (figure).

Herramientas utilizadas

El presente trabajo ha sido redactado por el autor usando LaTeX. El formato del texto es Computer Roman Modern a tamaño 11pt. Todos los gráficos e imágenes fueron incluidos en formato Encapsulated PostScript.

Nota sobre el copyright ®

Los derechos de cualquier marca comercial o registrada mencionada en el presente documento son propiedad de sus respectivos titulares.

Bibliography

[1] Leonard Flom and Aran Safir. Iris recognition system, United States patent 4.641.349, 1987.

[2] Lowe DG. Distinctive image features from scale-invariant key points. *Intl Journal of Computer Vision*, 60(2), 2004.

[3] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Trans. Circuits Syst. Video Techn.*, 14(1):4–20, 2004.

[4] Anil K. Jain, Arun Ross, and Salil Prabhakar. Biometrics: A tool for information security. *IEEE Trans. on Information Forensics and Security*, 1(2):125–143, 2006.

[5] B. Schneier. The uses and abuses of biometrics. page 136, 1999.

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle. An analysis of minutiae matching strength. *Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA*, LNCS-2091:223–228, 2001.

[7] John Daugman. How iris recognition works. *IEEE Trans. on Circuits and Systems for Video Technology*, 14:21–30, 2004.

[8] Craig Belcher and Yingzi Du. Region-based SIFT approach to iris recognition. *Optics and Lasers in Engineering*, 47(1), 2009.

[9] Kevin W. Bowyer, Karen Hollingsworth, and Patrick J. Flynn. Image understanding for iris biometrics: A survey. *Comput. Vis. Image Underst.*, 110(2):281–307, 2008.

[10] E. Grosso D.R. Kisku, A. Rattani and M. Tistarelli. Face identification by SIFT-based complete graph topology. *Proc. IEEE AUTOID*, 2007.

[11] Erina Takikawa Shihong Lao Masato Kawade Jun Luo, Yong Ma and Bao-Liang Lu. Person-specific SIFT features for face recognition. *Proc. IEEE ICASSP*, 2, 2007.

[12] S. Pankanti U. Park and A. K. Jain. Fingerprint verification using SIFT features. *Defense and Security Symposium, Biometric Technologies for Human Identification, BTHI, Proc. SPIE*, 2008.

[13] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez. Biosec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 40(4):1389–1392, 2007.

[14] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia. Direct attacks using fake images in iris verification. In *Proc. COST 2101 Workshop on Biometrics and Identity Management, BIOID, Roskilde, Denmark*, LNCS-5372, pages 181–190. Springer, May 2008.

[15] F. Alonso-Fernandez, P. Tome-Gonzalez, V. Ruiz-Albacete, and J. Ortega-Garcia. Iris recognition based on sift features. In *IEEE Proc. Intl. Conf. on Biometrics, Identity and Security, BIDS*, September 2009.

[16] A. Bertillon. La couleur de l'iris. *Rev. Sci. 36 (3)*, pages 65–73, 1885.

[17] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of Fingerprint Recognition.* Springer, New York, 2003.

[18] International Biometric Group. Biometric market and industry report 2009-2014, October 2008.

[19] C. Soutar, R. Gilroy, and A. Stoianov. Biometric system performance and security. *Proc. IEEE Workshop on Automatic Identification Advanced Technologies, AIAT*, -:–, 1999.

[20] C. Fancourt, L. Bogoni, K. Hanna, Y. Guo, R. Wildes, N. Takahashi, and U. Jain. Iris recognition at a distance. *Conf. on Audio- and Video-Based Biometric Person Authentication, IAPR*, LNCS-3546:1–13, 2005.

[21] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. *Handbook of Multibiometrics (International Series on Biometrics).* Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[22] John Daugman. Available from: <http://www.cl.cam.ac.uk/jgd1000/>.

[23] John G. Daugman. Biometric personal identification system based on iris analysis, United States patent 5.291.560, 1994.

[24] Wildes et al. Automated, non-invasive iris recognition system and method, United States patent 5.572.596, 1996.

[25] E.M. Newton and P.J. Phillips. Meta-analysis of third party evalutions of iris recognition. *IEEE Trans. SMC-A*, 1:39, 2009.

[26] Yingzi Eliza Du. Review of iris recognition: cameras, systems, and their applications. *Sensor review*, Emeral Group-26/1:66–69, 2006.

[27] Iridian Technology. Available from: <http://www.iriscan.com/>.

[28] J.R. Matey, O.Ñaroditsky, K. Hanna, R. Kolczynski, D.J. LoIacono, S. Mangru, M. Tinker, T.M. Zappia, and W.Y. Zhao. Iris on the move: Acquisition of images for iris recognition in less constrained environments. *Proceedings of the IEEE*, 94(11):1936–1947, Nov. 2006.

[29] J.R. Beveridge W.T. Scruggs A.J. O'Tooles D. Bolme K.W. Bowyer B.A. Draper G.H. Givens Y.M. Lui H. Sahibzada J.A. Scallan III P.J. Philips, P.J. Flynn and S. Weimers. Overview of the multiple biometrics grand challenge. *Proceedings of ICB, Springer LNCS-5558, Alghero (Italy)*, 2009.

[30] R.J. Micheals Y. Lee, P.J. Philips. An automated video-based system for iris recognition. *Proceedings of ICB, Springer LNCS-5558, Alghero (Italy)*, 2009.

[31] C.H. Kuo G. Medioni, J. Choi and D. Fidaleo. Identifying noncooperative subjects at a distance using face images and inferred 3d face models. *IEEE Trans SMC-A*, 1:39, 2009.

[32] J. Daugman. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 15(11):1148–1161, 1993.

[33] T.A. Camus and R. Wildes. Reliable and fast eye finding in close-up images. *Pattern Recognition, 2002. Proceedings. 16th International Conference on*, 1:389–394 vol.1, 2002.

[34] C. Sanchez-Avila, R. Sanchez-Reillo, and D. de Martin-Roche. Iris-based biometric recognition using dyadic wavelet transform. *Aerospace and Electronic Systems Magazine, IEEE*, 17(10):3–6, Oct 2002.

[35] V. Dorairaj, N.A. Schmid, and G. Fahmy. Performance evaluation of non-ideal iris based recognition system implementing global ica encoding. *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, 3:III–285–8, 11-14 Sept. 2005.

[36] R. Wildes. Iris recognition: an emerging biometric technology. *Proceedings of IEEE*, 85(9), 1997.

[37] Yuanning Liu, Senmiao Yuan, Xiaodong Zhu, and Qingliang Cui. A practical iris acquisition system and a fast edges locating algorithm in iris recognition. *Instrumentation and Measurement Technology Conference, 2003. IMTC '03. Proceedings of the 20th IEEE*, 1:166–168, 20-22 May 2003.

[38] Ya-Ping Huang, Si-Wei Luo, and En-Yi Chen. An efficient iris recognition system. *Machine Learning and Cybernetics, 2002. Proceedings. 2002 International Conference on*, 1:450–454 vol.1, 2002.

[39] Hanho Sung, Jaekyung Lim, Ji hyun Park, and Yillbyung Lee. Iris recognition using collarette boundary localization. In *ICPR (4)*, pages 857–860, 2004.

[40] Pan Lili and Xie Mei. The algorithm of iris image preprocessing. In *AUTOID '05: Proceedings of the Fourth IEEE Workshop on Automatic Identification Advanced Technologies*, pages 134–138, Washington, DC, USA, 2005. IEEE Computer Society.

[41] XiaoFu He and Pengfei Shi. A novel iris segmentation method for hand-held capture device. In *ICB*, pages 479–485, 2006.

[42] Qi-Chuan Tian, Quan Pan, Yong-Mei Cheng, and Quan-Xue Gao. Fast algorithm and application of hough transform in iris segmentation. *Machine Learning and Cybernetics, 2004. Proceedings of 2004 International Conference on*, 7:3977–3980 vol.7, Aug. 2004.

[43] Amjad Zaim, Mahmoud K. Quweider, Jeff Scargle, Juan Iglesias, and R. Tang. A robust and accurate segmentation of iris images using optimal partitioning. In *ICPR (4)*, pages 578–581, 2006.

[44] GuangZhu Xu, ZaiFeng Zhang, and Yide Ma. Automatic iris segmentation based on local areas. In *ICPR (4)*, pages 505–508, 2006.

[45] Caitang Sun, Chunguang Zhou, Yanchun Liang, and Xiangdong Liu. Study and improvement of iris location algorithm. In *ICB*, pages 436–442, 2006.

[46] B. Bonney, R. Ives, D. Etter, and Yingzi Du. Iris pattern extraction using bit planes and standard deviations. *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, 1:582–586 Vol.1, 7-10 Nov. 2004.

[47] H.M. El-Bakry. Fast iris detection for personal identification using modular neural networks. *Circuits and Systems, 2001. ISCAS 2001. The 2001 IEEE International Symposium on*, 3:581–584 vol. 2, 6-9 May 2001.

[48] Zhaofeng He, Tieniu Tan, and Zhenan Sun. Iris localization via pulling and pushing. In *ICPR '06: Proceedings of the 18th International Conference on Pattern Recognition*, pages 366–369, Washington, DC, USA, 2006. IEEE Computer Society.

[49] Paul A. Viola and Michael J. Jones. Robust real-time object detection. In *International Journal of Computer Vision*, page 747, 2001.

[50] Mihran Tucceryan. Moment-based texture segmentation. *Pattern Recogn. Lett.*, 15(7):659–668, 1994.

[51] Xin Li. Modeling intra-class variation for nonideal iris recognition. In *ICB*, pages 419–427, 2006.

[52] Aditya Abhyankar, Lawrence Hornak, and Stephanie A. C. Schuckers. Off-angle iris recognition using bi-orthogonal wavelet network system. In *AutoID*, pages 239–244, 2005.

[53] V. Dorairaj, N.A. Schmid, and G. Fahmy. Performance evaluation of non-ideal iris based recognition system implementing global ica encoding. *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, 3:III–285–8, 11-14 Sept. 2005.

[54] Aditya Abhyankar and Stephanie Schuckers. Active shape models for effective iris segmentation. In *SPIE 6202: Biometric Technology for Human Identification III*, pages 6202:H1–H10, 2006.

[55] Cecilia Di Ruberto, Sergio Vitulano, and Giuseppe Rodriguez. Image segmentation by texture analysis. *ICIAP*, pages 376–381, 1999.

[56] Olga Veksler. Image segmentation by nested cuts. *In IEEE Conference on Computer Vision and Pattern Recognition*, pages 339–344, 2000.

[57] Adams Wai-Kin Kong and David Zhang. Detecting eyelash and reflection for accurate iris segmentation. *IJPRAI*, 17(6):1025–1034, 2003.

[58] Junzhou Huang, Yunhong Wang, Tieniu Tan, and Jiali Cui. A new iris segmentation method for recognition. *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, 3:554–557 Vol.3, 23-26 Aug. 2004.

[59] Junzhou Huang, Yunhong Wang, Jiali Cui, and Tieniu Tan. Noise removal and impainting model for iris image. *Image Processing, 2004. ICIP '04. 2004 International Conference on*, 2:869–872 Vol.2, 24-27 Oct. 2004.

[60] Asheer Kasar Bachoo and Jules-Raymond Tapamo. Texture detection for segmentation of iris images. In *SAICSIT '05: Proceedings of the 2005 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, pages 236–243, , Republic of South Africa, 2005. South African Institute for Computer Scientists and Information Technologists.

[61] L. Masek et al. *Recognition of human iris patterns for biometric identification.* PhD thesis, Technical Report, The school of Computer Science and Software Engineering, The University of Western Australia, 2003.

[62] H. Proenca and L.A. Alexandre. Iris segmentation methodology for non-cooperative recognition. *Vision, Image and Signal Processing, IEE Proceedings -*, 153(2):199–205, 6 April 2006.

[63] J. Daugman. How iris recognition works. *Proceedings of 2002 International Conference on Image Processing*, 1:22–25, 2002.

[64] R.P. Wildes, J.C. Asmuth, G.L. Green, S.C. Hsu, R.J. Kolczynski, J.R. Matey, and S.E. McBride. A system for automated iris recognition. *Applications of Computer Vision, 1994., Proceedings of the Second IEEE Workshop on*, pages 121–128, 5-7 Dec 1994.

[65] W.W. Boles and B. Boashash. A human identification technique using images of the iris and wavelet transform. *Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on]*, 46(4):1185–1188, Apr 1998.

[66] R. Sánchez Reíllo C.Sánchez Ávila. *Tecnologías biométricas aplicadas a la seguridad.* Capitulo 5:"Iris y Retina", 2005.

[67] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang. Personal identification based on iris texture analysis. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 25(12):1519–1533, Dec. 2003.

[68] A.V. Oppenheim and J.S. Lim. The importance of phase in signals. *Proceedings of the IEEE*, 69(5):529–541, May 1981.

[69] David J. Field. Relations between the statistics of natural images and the response properties of cortical cells. *J. Opt. Soc. Am. A*, 4(12):2379, 1987.

[70] E. Rydgren, E.A. Thomas, F. Amiel, F. Rossant, and A. Amara. Iris features extraction using wavelet packets. *Image Processing, 2004. ICIP '04. 2004 International Conference on*, 2:861–864 Vol.2, 24-27 Oct. 2004.

[71] F. Rossant, M.T. Eslava, E.A. Thomas, F. Amiel, and A. Amara. Iris identification and robustness evaluation of a wavelet packets based algorithm. *Image Processing, 2005. ICIP 2005. IEEE International Conference on*, 3:III–257–60, 11-14 Sept. 2005.

[72] E. Krichen, M.A. Mellakh, S. Garcia-Salicetti, and B. Dorizzi. Iris identification using wavelet packets. *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, 4:335–338 Vol.4, 23-26 Aug. 2004.

[73] Jason Thornton, Marios Savvides, and B. V. K. Vijaya Kumar. An evaluation of iris pattern representations. *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on*, pages 1–6, 27-29 Sept. 2007.

[74] Lee K. Byeon O. Lim, S. and T. Kim. Efficient iris recognition through improvement of feature vector and classifier. *ETRI*, 23(2):61–70, 2001.

[75] Donald M. Monro, Soumyadip Rakshit, and Dexin Zhang. Dct-based iris recognition. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 29(4):586–595, April 2007.

[76] P. Burt and E. Adelson. The laplacian pyramid as a compact image code. *Communications, IEEE Transactions on [legacy, pre - 1988]*, 31(4):532–540, Apr 1983.

[77] Carmen Sanchez-Avila and Raul Sánchez-Reillo. Two different approaches for iris recognition using gabor filters and multiscale zero-crossing representation. *Pattern Recognition*, 38(2):231–240, 2005.

[78] Ons Abdel Alim and Maha Sharkas. Iris recognition using discrete wavelet transform and artificial neural net. *International Midwest Symposium on Circuits and Systems*, (1):337–340, 2003.

[79] Natalia A. Schmid Vivekanand Dorairaj and Gamal Fahmy. Performance evaluation of iris based recognition system implementing pca and ica encoding techniques. *SPIE 5779: Biometric Technology for Human Identification*, 5779.

[80] Yunhong Wang ong Zhu, Tieniu Tan. Biometric personal identification based on iris patterns. *ICPR2000: the 15th International Conference on Pattern Recognition*, 2000.

[81] Anti spoofing liveness detection. Available on line at <http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf>.

[82] Czajka A. Pacut, A. Aliveness detection for iris biometrics. *Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST*, pages 122–129, 2006.

[83] Masakatsu Nishigaki and Daisuke Arai. A user authentication based on human reflexes using blind spot and saccade response. *International Journal of Biometrics*, 1(2):173–190, 2008.

[84] M.Y. Javed A. Basit. Localization of iris in gray scale images using intensity gradient. *Optics and Lasers in Engineering*, 45(12):1107–1114, 2007.

[85] Byung Jun Kang and Kang Ryoung Park. A robust eyelash detection based on iris focus assessment. *Pattern Recogn. Lett.*, 28(13):1630–1639, 2007.

[86] Yi Chen, Sarat C. Dass, and Anil K. Jain. Localized iris image quality using 2-d wavelets. In *ICB*, pages 373–381, 2006.

[87] Nathan D. Kalka, Jinyu Zuo, Natalia A. Schmid, and Bojan Cukic. Image quality assessment for iris biometric. In *SPIE 6202 Biometric Technology for Human Identification III*, pages 6202:D1–D11, 2006.

[88] Iris Challenger Evaluation. Available from: <http://www.nist.gov/ICE/>.

[89] National Institute of Standars and Technology. Available from: <http://www.nist.gov/>.

[90] Brown M and Lowe DG. Invariant features from interest point groups. *British machine vision conference*, pages 656–665, 2002.

[91] K. Mikolajczyk. *Detection of local features invariant to affines transformations.* PhD thesis, INPG, 2002.

[92] L. Masek and P. Kovesi. Matlab source code for a biometric identification system based on iris patterns. *The School of Computer Science and Software Engineering, The University of Western Australia*, 2003.

[93] A.K. Jain, K.Ñandakumar, and A. Ross. Score Normalization in Multimodal Biometric Systems. *Pattern Recognition*, 38(12):2270–2285, December 2005.

[94] NIST MBGC. *NIST Multiple Biometric Grand Challenge - http://face.nist.gov/mbgc*, 2007.

Presupuesto

1) **Ejecución Material**	
▪ Compra de ordenador personal (Software incluido)	2.000 €
▪ Alquiler de impresora láser durante 6 meses	250 €
▪ Material de oficina	150 €
▪ Total de ejecución material	2.410 €
2) **Gastos generales**	
▪ sobre Ejecución Material	352 €
3) **Beneficio Industrial**	
▪ sobre Ejecución Material	132 €
4) **Honorarios Proyecto**	
▪ 1800 horas a 15 €/ hora	27000 €
5) **Material fungible**	
▪ Gastos de impresión	280 €
▪ Encuadernación	200 €
6) **Subtotal del presupuesto**	
▪ Subtotal Presupuesto	32.774 €
7) **I.V.A. aplicable**	
▪ 16 % Subtotal Presupuesto	5.243,8 €
8) **Total presupuesto**	
▪ Total Presupuesto	38.017,8 €

Madrid, Septiembre 2010

El Ingeniero Jefe de Proyecto

Fdo.: Virginia Ruiz Albacete

Ingeniero Superior de Telecomunicación

Pliego de condiciones

Pliego de condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un *Reconocimiento Biométrico de Iris Basado en Características SIFT*. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales.

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma,

por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad "Presupuesto de Ejecución de Contrata ^{2}anteriormente llamado "Presupuesto de Ejecución Material"que hoy designa otro concepto.

Condiciones particulares.

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.

Imágenes ejemplo de las bases de datos

En este anexo de muestran ejemplos de imágenes de las base de datos utilizada, BioSec baseline, y la generada a partir de la misma, compuesta de iris falsos.

.1. BioSec - Baseline

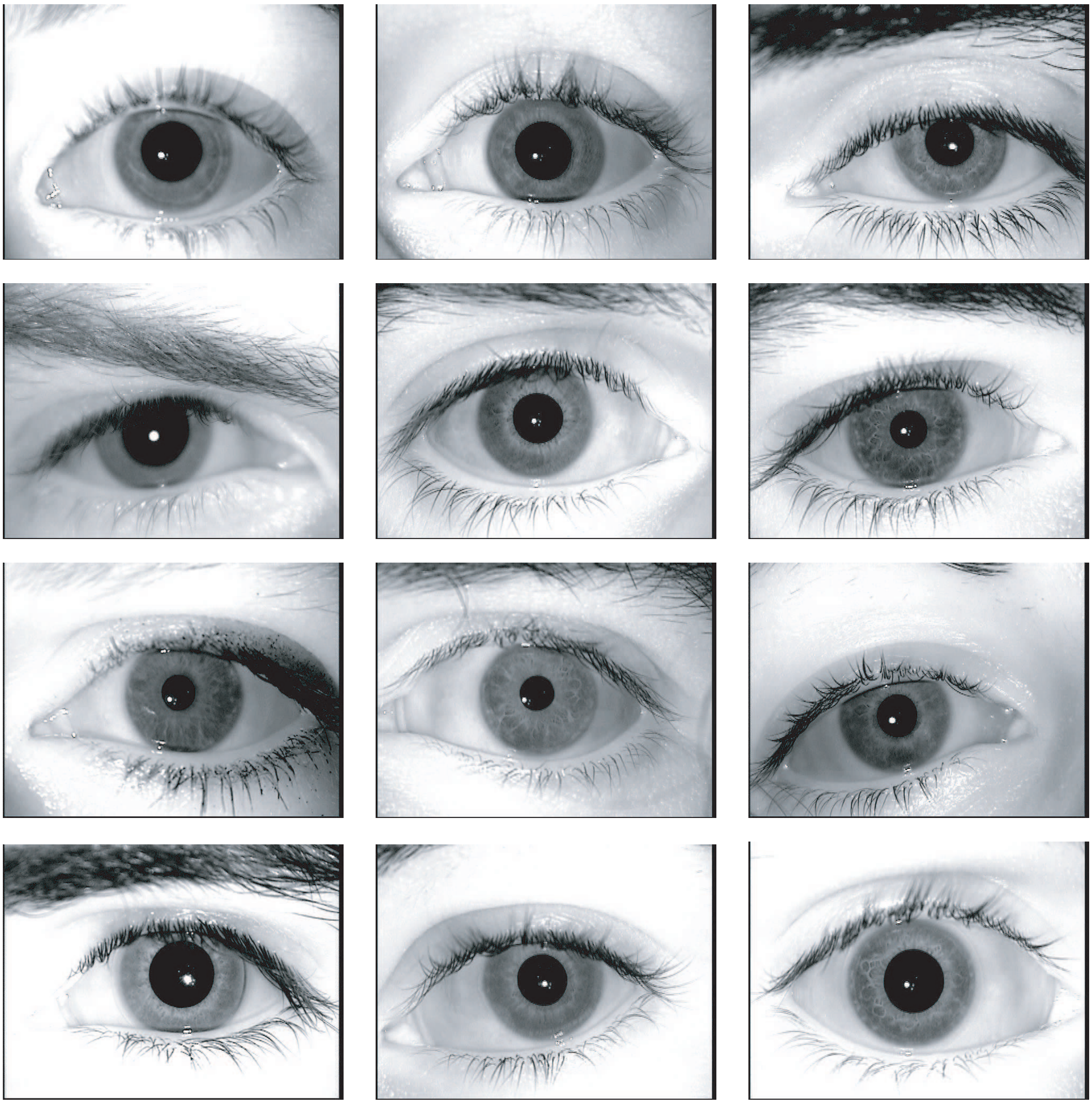


Figure 1: Example of the images in the BioSec Baseline database.

.2. BioSec - Fake

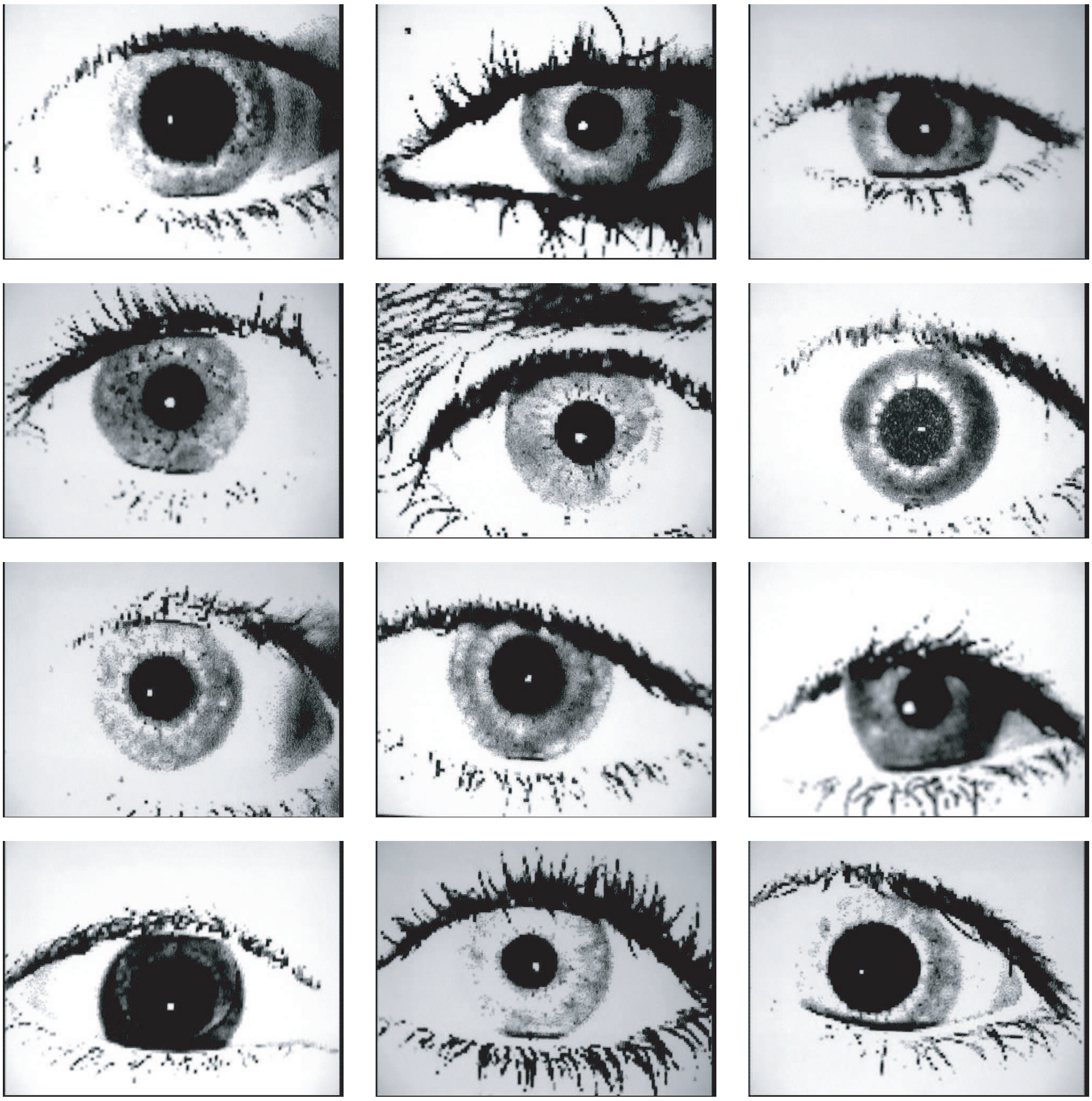


Figure 2: Example of the images found in the BioSec Develop Fake database.

Publications

Direct attacks using fake images in iris verification

Virginia Ruiz-Albacete, Pedro Tome-Gonzalez, Fernando Alonso-Fernandez,
Javier Galbally, Julian Fierrez, and Javier Ortega-Garcia

Biometric Recognition Group - ATVS
Escuela Politecnica Superior - Universidad Autonoma de Madrid
Avda. Francisco Tomas y Valiente, 11 - Campus de Cantoblanco
28049 Madrid, Spain - http://atvs.ii.uam.es
{virginia.ruiz, pedro.tome, fernando.alonso, javier.galbally,
julian.fierrez, javier.ortega}@uam.es

Abstract. In this contribution, the vulnerabilities of iris-based recognition systems to direct attacks are studied. A database of fake iris images has been created from real iris of the BioSec baseline database. Iris images are printed using a commercial printer and then, presented at the iris sensor. We use for our experiments a publicly available iris recognition system, which some modifications to improve the iris segmentation step. Based on results achieved on different operational scenarios, we show that the system is vulnerable to direct attacks, pointing out the importance of having countermeasures against this type of fraudulent actions.

Key words: Biometrics, iris recognition, direct attacks, fake iris

1 Introduction

The increasing interest on biometrics is related to the number of important applications where a correct assessment of identity is a crucial point. The term *biometrics* refers to automatic recognition of an individual based on anatomical (e.g., fingerprint, face, iris, hand geometry, ear, palmprint) or behavioral characteristics (e.g., signature, gait, keystroke dynamics) [1]. Biometric systems have several advantages over traditional security methods based on something that you know (password, PIN) or something that you have (card, key, etc.). In biometric systems, users do not need to remember passwords or PINs (which can be forgotten) or to carry cards or keys (which can be stolen). Among all biometric techniques, iris recognition has been traditionally regarded as one of the most reliable and accurate biometric identification system available [2]. Additionally, the iris is highly stable over a person's lifetime and lends itself to noninvasive identification because it is an externally visible internal organ [3].

However, in spite of these advantages, biometric systems have some drawbacks [4]: *i*) the lack of secrecy (e.g. everybody knows our face or could get our fingerprints), and *ii*) the fact that a biometric trait can not be replaced (if we forget a password we can easily generate a new one, but no new fingerprint can be generated if an impostor "steals" it). Moreover, biometric systems are vulnerable to external attacks which could decrease their level of security. In [5] Ratha *et al.* identified and classified eight possible attack points to biometric recognition systems. These vulnerability points, depicted in Figure 1, can broadly be divided into two main groups:

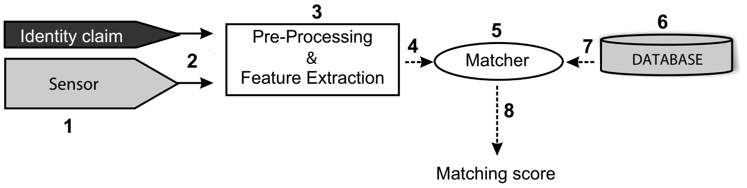


Fig. 1. Architecture of an automated biometric verification system. Possible attack points are numbered from 1 to 8.

- **Direct attacks**. Here, the sensor is attacked using synthetic biometric samples, e.g. gummy fingers (point 1 in Figure 1). It is worth noting that in this type of attacks no specific knowledge about the system is needed. Furthermore, the attack is carried out in the analog domain, outside the digital limits of the system, so digital protection mechanisms (digital signature, watermarking, etc) cannot be used.

- **Indirect attacks**. This group includes all the remaining seven points of attack identified in Figure 1. Attacks 3 and 5 might be carried out using a Trojan Horse that bypasses the system modules. In attack 6, the system database is manipulated. The remaining points of attack (2, 4, 7 and 8) exploit possible weak points in the communication channels of the system. In opposition to direct attacks, in this case the intruder needs to have some additional information about the internal working of the system and, in most cases, physical access to some of the application components. Most of the works reporting indirect attacks use some type of variant of the hill climbing technique introduced in [6].

In this work we concentrate our efforts in studying direct attacks on iris-based verification systems. For this purpose we have built a database with synthetic iris images generated from 50 users of the BioSec multi-modal baseline corpus [7]. This paper is structured as follows. In Sect. 2 we detail the process followed for the creation of the fake iris, and the database used in the experiments is presented. The experimental protocol, some results and further discussion are reported in Sect. 3. Conclusions are finally drawn in Sect. 4.

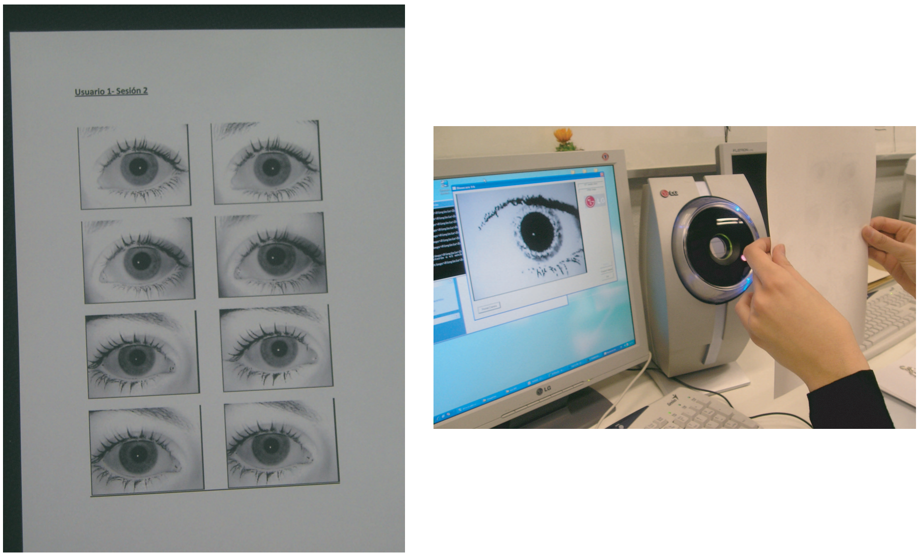


Fig. 2. Iris capture preparation.

PRINTER	PAPER	PREPROCESSING [8]
Ink Jet Laser	White paper Recycled paper Photographic paper High resolution paper Butter paper Cardboard	Histogram equalization Noise filtering Open/close Top hat

Table 1. Options tested for fake iris generation.

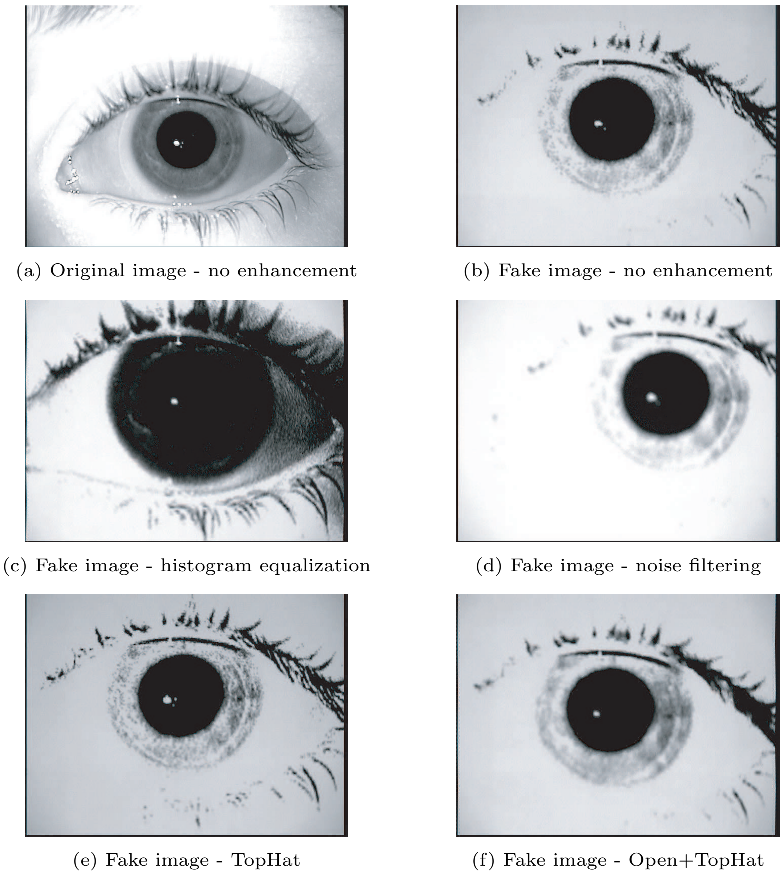
2 Fake Iris Database

A new iris database has been created using iris images from 50 users of the BioSec baseline database [7]. The process is divided into three steps: *i*) first original images are preprocessed for a better afterwards quality, then *ii*) they are printed on a piece of paper using a commercial printer as shown in Figure 2 (left), and lastly, *iii*) printed images are presented at the iris sensor, as can be seen in Figure 2 (right), obtaining the fake image.

2.1 Fake iris generation method

To correctly create a new database, it is necessary to take into account factors affecting the quality of acquired fake images. The main variables with significant importance for iris quality are found to be: preprocessing of original images, printer type and paper type.

We tested two different printers: a HP Deskjet 970cxi (inkjet printer) and a HP LaserJet 4200L (laser printer). They both give fairly good quality. On



(a) Original image - no enhancement

(b) Fake image - no enhancement

(c) Fake image - histogram equalization

(d) Fake image - noise filtering

(e) Fake image - TopHat

(f) Fake image - Open+TopHat

Fig. 3. Acquired fake images with different modifications using high quality paper and inkjet printer.

the other hand, we observed that the quality of acquired fake images depends on the type of paper used. Here comes the biggest range of options. All the tested types appear in Table 1. In our experiments, the preprocessing is specially important since it has been observed that the iris camera does not capture original images printed without previous modifications. Therefore we have tested different enhancement methods before printing in order to acquire good quality fake images. The options tested are also summarized in Table 1. By analyzing all the possibilities with a small set of images, the combination that gives the best segmentation results and therefore the best quality for the afterwards comparison has been found to be the inkjet printer, with high resolution paper and an Open-TopHat preprocessing step. In Figure 3, examples using different preprocessing techniques with this kind of paper and inkjet printer are shown.

2.2 Database

The fake iris database follows the same structure of the original BioSec database. Therefore, data for the experiments consists of 50 users × 2 eyes × 4 images × 2 sessions = 800 fake iris images, and its corresponding real images. Acquisition of fake images has been carried out with the same iris camera used in BioSec, a LG IrisAccess EOU3000.

3 Experiments

3.1 Recognition system

We have used for our experiments the iris recognition system[1] developed by Libor Masek [9]. It consists of the following sequence of steps that are described next: segmentation, normalization, encoding and matching.

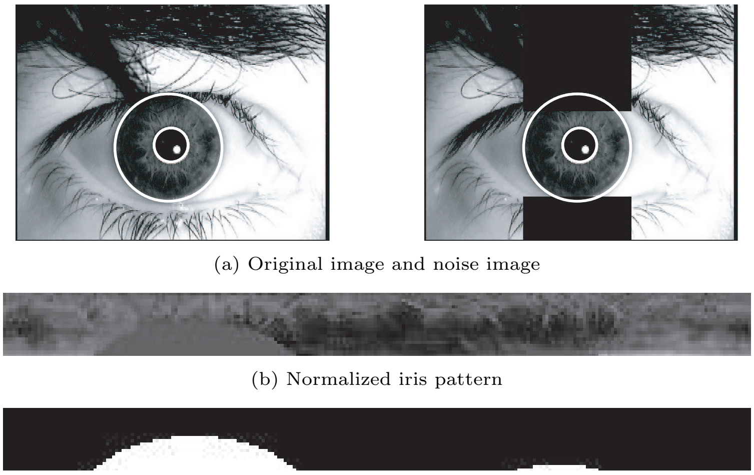
For iris segmentation, the system uses a circular Hough transform in order to detect the iris and pupil boundaries. Iris boundaries are modeled as two circles. The system also performs an eyelids removal step. Eyelids are isolated first by fitting a line to the upper and lower eyelid using a linear Hough transform (see Figure 4(a) right, in which the eyelid lines correspond to the border of the black blocks). Eyelashes detection by histogram thresholding is available in the source code, but it is not performed in our experiments. Although eyelashes are quite dark compared with the surrounding iris region, other iris areas are equally dark due to the imaging conditions. Therefore, thresholding to isolate eyelashes would also remove important iris regions. However, eyelash occlusion has been found to be not very prominent in our database.

To improve the performance of this segmentation procedure, we pre-estimate the iris centroid by histogram thresholding, since iris region is observed to have the lowest gray levels of an iris image. This pre-estimation allows to reduce the searching area of the circular Hough transform. Also, we impose three conditions to the two circles that model iris and pupil boundaries: *i*) although these two circles are known to be non-concentric, a maximum value is imposed to the distance among their centers; *ii*) the two circles are not allowed to to have parts outside the iris image; and *iii*) the radius of the two circles are not allowed to be similar.

Normalization of iris regions is performed using a technique based on Daugman's rubber sheet model [10]. The center of the pupil is considered as the reference point, based on which a 2D array is generated consisting of an angular-radial mapping of the segmented iris region. In Figure 4, an example of the normalization step is depicted.

Feature encoding is implemented by convolving the normalized iris pattern with 1D Log-Gabor wavelets. The rows of the 2D normalized pattern are taken as the 1D signal, each row corresponding to a circular ring on the iris region. It

[1] The source code can be freely downloaded from `www.csse.uwa.edu.au/~pk/studentprojects/libor/sourcecode.html`



(a) Original image and noise image

(b) Normalized iris pattern

(c) Noise mask

Fig. 4. Examples of the normalization step.

uses the angular direction since maximum independence occurs in this direction. The filtered output is then phase quantized to four levels using the Daugman method [10], with each filtering producing two bits of data. The output of phase quantization is a grey code, so that when going from one quadrant to another, only 1 bit changes. This will minimize the number of bits disagreeing, if say two intra-class patterns are slightly misaligned and thus will provide more accurate recognition [9]. The encoding process produces a binary template and a corresponding noise mask which represents the eyelids areas (see Figure 4 (c)).

For matching, the Hamming distance is chosen as a metric for recognition. The Hamming distance employed incorporates the noise mask, so that only significant bits are used in calculating the Hamming distance between two iris templates. The modified Hamming distance formula is given by

$$HD = \frac{1}{N - \sum_{k=1}^{N} Xn_k (OR) Yn_k} \cdot \sum_{j=1}^{N} X_j (XOR) Y_j (AND) Xn'_j (AND) Yn'_j$$

where X_j and Y_j are the two bitwise templates to compare, Xn_j and Yn_j are the corresponding noise masks for X_j and Y_j, and N is the number of bits represented by each template.

In order to account for rotational inconsistencies, when the Hamming distance of two templates is calculated, one template is shifted left and right bitwise and a number of Hamming distance values are calculated from successive shifts [10]. This method corrects for misalignments in the normalized iris pattern caused by rotational differences during imaging. From the calculated distance values, the lowest one is taken.

3.2 Experimental Protocol

For the experiments, each eye in the database is considered as a different user. In this way, we have two sessions with 4 images each for 100 users (50 donors × 2 eyes per donor).

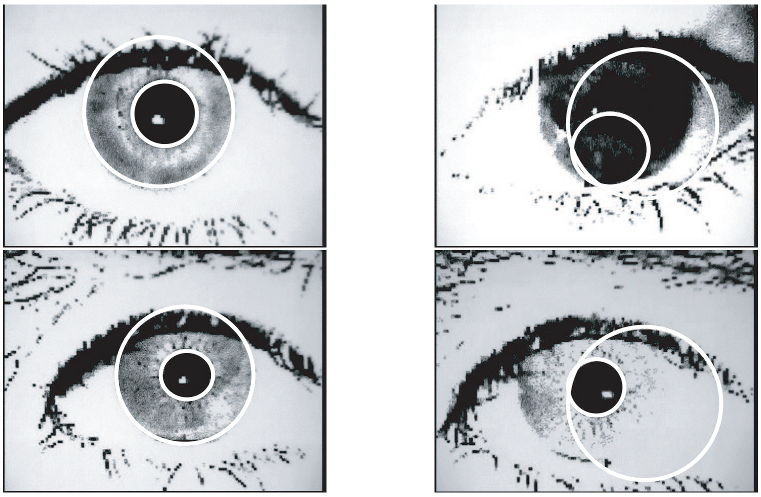
Two different attack scenarios are considered in the experiments and compared to the system normal operation mode:

- **Normal Operation Mode (NOM)**: both the enrollment and the test are carried out with a real iris. This is used as the reference scenario. In this context the FAR (False Acceptance Rate) of the system is defined as the number of times an impostor using his own iris gains access to the system as a genuine user, which can be understood as the robustness of the system against a zero-effort attack. The same way, the FRR (False Rejection Rate) denotes the number of times a genuine user is rejected by the system.
- **Attack 1**: both the enrollment and the test are carried out with a fake iris. In this case the attacker enrolls to the system with the fake iris of a genuine user and then tries to access the application also with a fake iris of the same user. In this scenario an attack is unsuccessful (i.e. the system repels the attack) when the impostor is not able to access the system using the fake iris. Thus, the attack success rate (SR) in this scenario can be computed as: $\mathrm{SR} = 1 - \mathrm{FRR}$.
- **Attack 2**: the enrollment is performed using a real iris, and tests are carried out with fake iris. In this case the genuine user enrolls with his/her iris and the attacker tries to access the application with the fake iris of the legal user. A successful attack is accomplished when the system confuses a fake iris with its corresponding genuine iris, i.e., $\mathrm{SR} = \mathrm{FAR}$.

In order to compute the performance of the system in the normal operation mode, the experimental protocol is as follows. For a given user, all the images of the first session are considered as enrolment templates. Genuine matchings are obtained by comparing the templates to the corresponding images of the second session from the same user. Impostor matchings are obtained by comparing one randomly selected template of a user to a randomly selected iris image of the second session from the remaining users. Similarly, to compute the FRR in attack 1, all the fake images of the first session of each user are compared with the corresponding fake images of the second session. In the attack 2 scenario, only the impostor scores are computed matching all the 4 original samples of each user with its 4 fake samples of the second session. In our experiments, not all the images were segmented successfully by the recognition system. As a result, it was not possible to use all the eye images for testing experiments.

3.3 Results

In Figure 5, several examples of fake images with correct and incorrect iris detection are plotted. The number of correctly segmented images are 792 for the original database (99% of the 800 available) and 574 for the fake database (71.75%



(a) Correct iris detection

(b) Incorrect iris detection

Fig. 5. Examples of fake images with correct iris detection (left) and incorrect iris detection (right).

of the 800). It is worth noting than more than 70% of fake images pass through the segmentation and normalization stages, and they are input into the feature extraction and matching stages. Thanks to the modifications included in the segmentation stage (see Section 3.1), we have improved the segmentation rate of the original system, which in our preliminary experiments was 80.56% and 38.43% for the original and fake database, respectively. It is important to consider that as we try to improve the segmentation rate of true iris images, we are also improving the segmentation rate of fake images.

In Table 2 we show the Success Rate (SR) of the direct attacks against the recognition system at four different operating points, considering only the matchings between correctly segmented images. The decision threshold is fixed to reach a FAR={0.1, 1, 2, 5} % in the normal operation mode (NOM), and then the success rate of the two proposed attacks is computed. We observe that in all the operating points, the system is vulnerable to the two attacks (i.e. a success rate of about 35% or higher is observed). This is specially evident as the FAR in the normal operation mode is increased, being successful more than half of the attacks. It is also remarkable the high success rates observed for attack 1, which are quite similar to attack 2. In the attack 1, an intruder would be correctly enrolled in the system using a fake image of another person and at a later date, he/she would be granted access to the system also using a fake image.

NOM	**Attack 1**	**Attack 2**
FAR - FRR (%)	SR (%)	SR (%)
0.1 - 16.84	33.57	36.89
1 - 12.37	48.02	52.44
2 - 10.78	53.03	56.96
5 - 8.87	61.19	64.56

Table 2. Evaluation of the verification system to direct attacks. NOM refers to the system normal operation mode and SR to the success rate of the attack.

4 Conclusion

An evaluation of the vulnerabilities to direct attacks of iris-based verification systems has been presented. The attacks have been evaluated using fake iris images created from real iris of the BioSec baseline database. We printed iris images with a commercial printer and then, we presented the images to the iris sensor. Different factors affecting the quality of acquired fake images have been studied, including preprocessing of original images, printer type and paper type. We have chosen the combination giving the best quality and then, we have built a database of fake images from 100 eyes, with 8 iris images per eye. Acquisition of fake images has been carried out with the same iris camera used in BioSec.

Two attack scenarios have been compared to the normal operation mode of the system using a publicly available iris recognition system. The first attack scenario considers enrolling to the system and accessing it with fake iris. The second one represents accessing a genuine account with fake iris. Results showed that the system is vulnerable to the two evaluated attacks. We also observed that about 72% of the fake images were correctly segmented by the system. When that this happens, the intruder is granted access with high probability, reaching the success rate of the two attacks a 50% or higher.

Liveness detection procedures are possible countermeasures against direct attacks. For the case of iris recognition systems, light reflections or behavioral features like eye movement, pupil response to a sudden lighting event, etc. have been proposed [11, 12]. This research direction will be the source of future work. We will also explore the use of another type of iris sensors, as the OKI's handheld iris sensor used in the CASIA database[2].

Acknowledgments. This work has been supported by Spanish project TEC2006-13141-C03-03, and by European Commission IST-2002-507634 Biosecure NoE. Author F. A.-F. is supported by a FPI Fellowship from Consejeria de Educacion de la Comunidad de Madrid. Author J. G. is supported by a FPU Fellowship from the Spanish MEC. Author J. F. is supported by a Marie Curie Fellowship from the European Commission.

[2] http://www.cbsr.ia.ac.cn/databases.htm

References

1. Jain, A., Ross, A., Pankanti, S.: Biometrics: A tool for information security. IEEE Trans. on Information Forensics and Security **1** (2006) 125–143
2. Jain, A., Bolle, R., Pankanti, S., eds.: Biometrics - Personal Identification in Networked Society. Kluwer Academic Publishers (1999)
3. Monro, D., Rakshit, S., Zhang, D.: DCT-Based iris recognition. IEEE Trans. on Pattern Analysis and Machine Intelligence **29**(4) (April 2007) 586–595
4. Schneier, B.: The uses and abuses of biometrics. Communications of the ACM **48** (1999) 136
5. Ratha, N., Connell, J., Bolle, R.: An analysis of minutiae matching strength. Proc. International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA **Springer LNCS-2091** (2001) 223–228
6. Soutar, C., Gilroy, R., Stoianov, A.: Biometric system performance and security. Proc IEEE Workshop on Automatic Identification Advanced Technologies, AIAT (1999)
7. Fierrez, J., Ortega-Garcia, J., Torre-Toledano, D., Gonzalez-Rodriguez, J.: BioSec baseline corpus: A multimodal biometric database. Pattern Recognition **40**(4) (April 2007) 1389–1392
8. Gonzalez, R., Woods, R.: Digital Image Processing. Addison-Wesley (2002)
9. Masek, L., Kovesi, P.: Matlab source code for a biometric identification system based on iris patterns. The School of Computer Science and Software Engineering, The University of Western Australia (2003)
10. Daugman, J.: How iris recognition works. IEEE Transactions on Circuits and Systems for Video Technology **14** (2004) 21–30
11. Daugman, J.: Anti spoofing liveness detection. available on line at http://www.cl.cam.ac.uk/users/jgd1000/countermeasures.pdf
12. Pacut, A., Czajka, A.: Aliveness detection for iris biometrics. Proc. IEEE Intl. Carnahan Conf. on Security Technology, ICCST (2006) 122–129

Iris Recognition Based on SIFT Features

Fernando Alonso-Fernandez, Pedro Tome-Gonzalez, Virginia Ruiz-Albacete, Javier Ortega-Garcia

Abstract— **Biometric methods based on iris images are believed to allow very high accuracy, and there has been an explosion of interest in iris biometrics in recent years. In this paper, we use the Scale Invariant Feature Transformation (SIFT) for recognition using iris images. Contrarily to traditional iris recognition systems, the SIFT approach does not rely on the transformation of the iris pattern to polar coordinates or on highly accurate segmentation, allowing less constrained image acquisition conditions. We extract characteristic SIFT feature points in scale space and perform matching based on the texture information around the feature points using the SIFT operator. Experiments are done using the BioSec multimodal database, which includes 3,200 iris images from 200 individuals acquired in two different sessions. We contribute with the analysis of the influence of different SIFT parameters on the recognition performance. We also show the complementarity between the SIFT approach and a popular matching approach based on transformation to polar coordinates and Log-Gabor wavelets. The combination of the two approaches achieves significantly better performance than either of the individual schemes, with a performance improvement of 24% in the Equal Error Rate.**

I. INTRODUCTION

Recognizing people based on anatomical (e.g., fingerprint, face, iris, hand geometry, ear, palmprint) or behavioral characteristics (e.g., signature, gait, keystroke dynamics), is the main objective of biometric recognition techniques [1]. The increasing interest on biometrics is related to the number of important applications where a correct assessment of identity is a crucial point. Biometric systems have several advantages over traditional security methods based on something that you know (password, PIN) or something that you have (card, key, etc.). In biometric systems, users do not need to remember passwords or PINs (which can be forgotten) or to carry cards or keys (which can be stolen). Among all biometric techniques, iris recognition has been traditionally regarded as one of the most reliable and accurate biometric identification system available [2]. Additionally, the iris is highly stable over a person's lifetime and lends itself to noninvasive identification because it is an externally visible internal organ [3].

Traditional iris recognition approaches approximates iris boundaries as circles. The ring-shaped region of the iris is then transferred to a rectangular image in polar coordinates as shown in Figure 1, with the pupil center being the center of the polar coordinates [4]. This transfer normalizes the distance between the iris boundaries due to contraction/dilation of the pupil, the camera zoom or the camera to eye distance. When converting an iris region to polar coordinates, it is necessary a very accurate segmentation in order to create a similar iris pattern mapping between images of the same eye [5]. Features are then extracted from the rectangular normalized iris pattern. For this purpose, a number of approaches have been proposed in the literature [6], e.g.: Gabor filters, log-Gabor filters, Gaussian filters, Laplacian-of-Gaussian filters, wavelet transforms, etc.

One of the drawbacks of traditional iris recognition approaches is that the transformation to polar coordinates can fail with non-cooperative or low quality data (e.g. changes in the eye gaze, non-uniform illumination, eyelashes/eyelids occlusion, etc.) [5]. In this paper, we implement the Scale Invariant Feature Transformation (SIFT) [7] for its use in biometric recognition using iris images. SIFT extracts repeatable characteristic feature points from an image and generates descriptors describing the texture around the feature points. The SIFT technique has already demonstrated its efficacy in other generic object recognition problems, and it has been recently proposed for its use in biometric recognition systems based on face [8], [9], fingerprint [10] and iris images [5]. One of the advantages of the SIFT approach is that it does not need transfer to polar coordinates. We have used for our experiments the BioSec multimodal baseline corpus [11] which includes 3,200 iris images from 200 individuals acquired in two different sessions. We analyze the influence of different SIFT parameters on the verification performance, including the implementation of a technique to remove false matches, as proposed previously for fingerprints [10]. We also demonstrate that the proposed approach complements

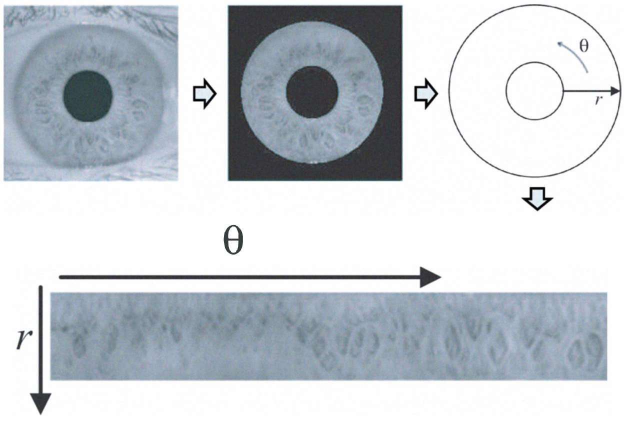


Fig. 1. Normalization of the iris region to polar coordinates. The ring-shaped region of the iris is transferred to a rectangular image, with the pupil center being the center of the polar coordinates.

Biometric Recognition Group - ATVS, Escuela Politecnica Superior, Universidad Autonoma de Madrid, Avda. Francisco Tomas y Valiente, 11, Campus de Cantoblanco, 28049 Madrid, Spain, email: {fernando.alonso, pedro.tome, virginia.ruiz, javier.ortega}@uam.es

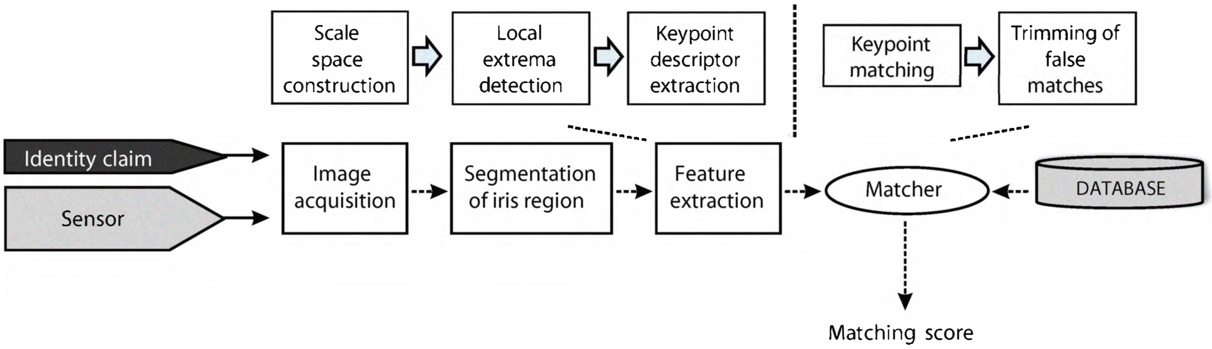


Fig. 2. Architecture of an automated iris verification system using the SIFT operator.

traditional iris recognition approaches based on transformation to polar coordinates and Log-Gabor wavelets [12], [13]. In our experiments, the fusion of the two techniques achieves a performance improvement of 24% in the Equal Error Rate.

Furthermore, since the SIFT technique does not require polar transformation or highly accurate segmentation, and it is invariant to changes in illumination, scale and rotation, it is hoped that this technique will be feasible with unconstrained image acquisition conditions. One of the major current practical limitations of iris biometrics is the degree of cooperation required on the part of the person whose image is to be acquired. All existing commercial iris biometrics systems still have constrained image acquisition conditions [6]. Current efforts are aimed at acquiring images in a more flexible manner and/or being able to use images of more widely varying quality, e.g. the "Iris on the Move" project [14], which is aimed to acquire iris images as a person walks at normal speed through an access control point such as those common at airports. This kind of systems would drastically reduce the need of user's cooperation, achieving transparent and low-intrusive biometric systems, with a higher degree of acceptance among users.

The rest of the paper is organized as follows. Section II describes the SIFT algorithm. Section III describes our experimental framework, including the database used, the protocol, and the results. Finally, conclusions and future work are drawn in Section IV.

II. SCALE INVARIANT FEATURE TRANSFORMATION (SIFT)

Scale Invariant Feature Transformation (SIFT) [7] was originally developed for general purpose object recognition. SIFT detects stable feature points of an object such that the same object can be recognized with invariance to illumination, scale, rotation and affine transformations. A brief description of the steps of the SIFT operator and their use in iris recognition is given next. The diagram of a iris recognition system using the SIFT operator is shown in Figure 2.

A. Scale-space local extrema detection

The first step is to construct a Gaussian scale space, which is done by convolving a variable scale 2D Gaussian operator $G(x, y, \sigma)$ with the input image $I(x, y)$:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \qquad (1)$$

Difference of Gaussian (DoG) images $D(x, y, \sigma)$ are then obtained by subtracting subsequent scales in each octave:

$$D(x, y, \sigma) = L(x, y, k\sigma) - L(x, y, \sigma) \qquad (2)$$

where k is a constant multiplicative factor in scale space. The set of Gaussian-smoothed images and DoG images are called an octave. A set of such octaves is constructed by successively down sampling the original image. Each octave (i.e., doubling of σ) is divided into an integer number s of scales, so $k = 2^{1/s}$. We must produce s+3 images for each octave, so that the final extrema detection covers a complete octave. In this paper we have used s=3, thus producing six Gaussian-smoothed images and five DOG images per octave, and a value of σ=1.6 (values from Lowe [7]). Figure 3 shows 3 successive octaves with 6 scales and the corresponding difference images.

Local extrema are then detected by observing each image point in $D(x, y, \sigma)$. A point is decided as a local minimum or maximum when its value is smaller or larger than all its surrounding neighboring points. Each sample point in $D(x, y, \sigma)$ is compared to its eight neighbors in the current image and nine neighbors in the scale above and below.

B. Accurate Keypoint Localization

Once a keypoint candidate has been found, if it observed to have low contrast (and is therefore sensitive to noise) or if it is poorly localized along an edge, it is removed because it can not be reliably detected again with small variation of viewpoint or lighting changes. Two thresholds are used, one to exclude low contrast points and other to exclude edge points. More detailed description of this process can be found in the original paper by Lowe [7].

C. Orientation assignment

An orientation histogram is formed from the gradient orientations within a 16×16 region around each keypoint. The orientation histogram has 36 bins covering the 360 degree range of orientations. Each sample added to the histogram

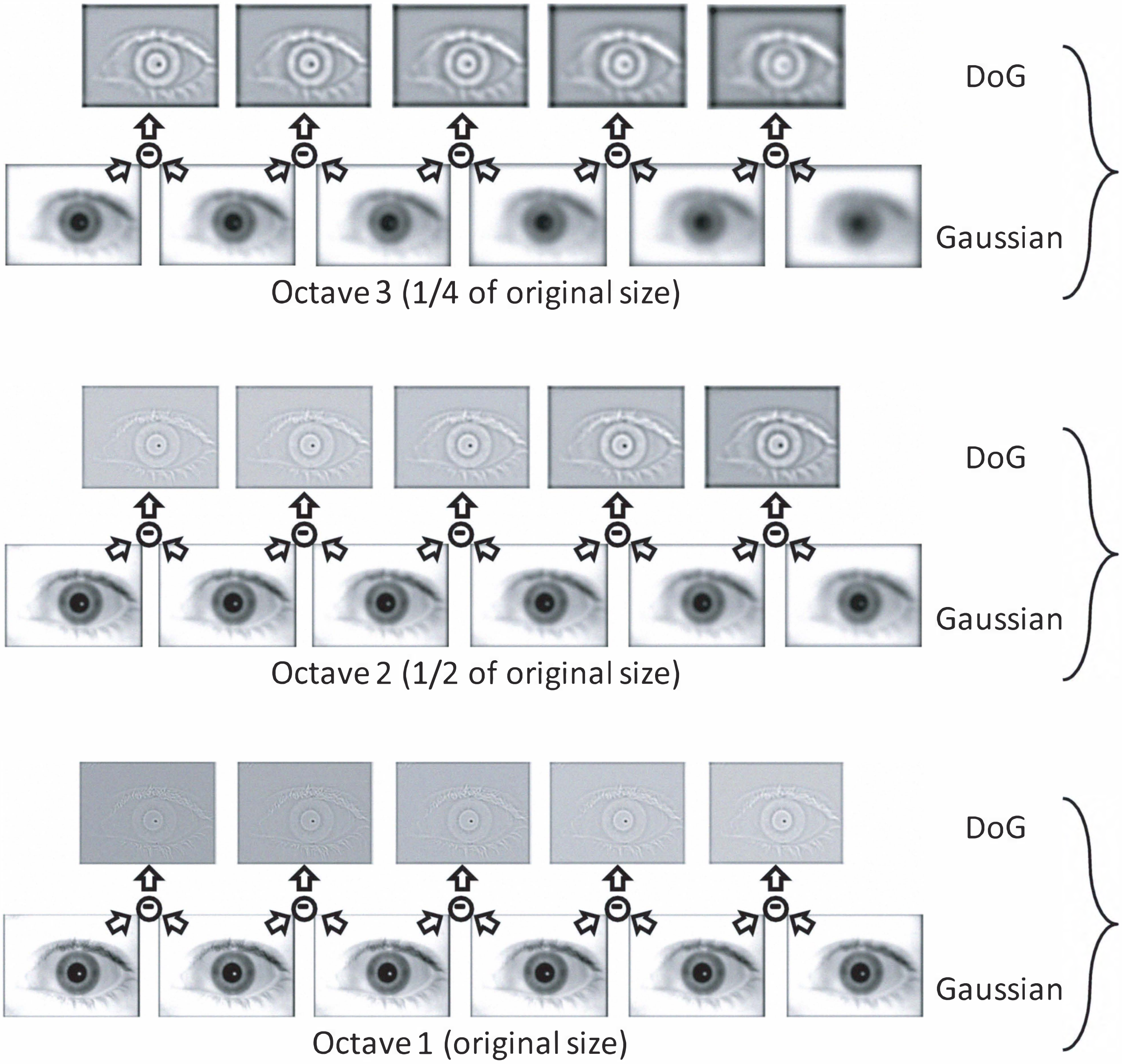

DoG
Gaussian
Octave 3 (1/4 of original size)
DoG
Gaussian
Octave 2 (1/2 of original size)
DoG
Gaussian
Octave 1 (original size)

Fig. 3. Example of SIFT scale space construction. The figure shows 3 successive octaves, with 6 scales per octave, and the corresponding difference images.

is weighted by its gradient magnitude and by a Gaussian-weighted circular window centered at the keypoint. The purpose of this Gaussian window is to give less emphasis to gradients that are far from the center of the local extremum.

The highest peak in the histogram is then detected, as well as any other local peak that is within 80% of the highest peak. For locations with multiple peaks, there will be multiple keypoints created at the same location, but with different orientations. The major orientations of the histogram are then assigned to the keypoint, so the keypoint descriptor can be represented relative to them, thus achieving invariance to image rotation.

D. Keypoint descriptor

In this stage, a distinctive descriptor is computed at each keypoint. The image gradient magnitudes and orientations, relative to the major orientation of the keypoint, are sampled within a 16×16 region around each keypoint. These samples are then accumulated into orientation histograms summarizing the contents over 4×4 subregions, as shown in Figure 4. Each orientation histogram has 8 bins covering the 360 degree range of orientations. Each sample added to the histogram is weighted by its gradient magnitude and by a Gaussian circular window centered at the local extremum. The descriptor is then formed from a vector containing the values of all the orientation histogram entries,

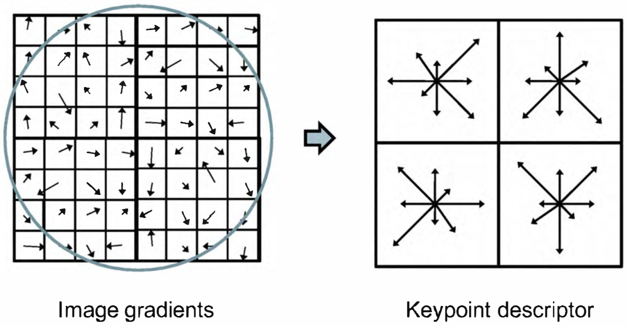


Fig. 4. Computation of SIFT keypoint descriptor (image from [7]). The gradient magnitude and orientation at each image sample point in a region around the keypoint location is first computed, as shown on the left, weighted by a Gaussian window (indicated by the overlaid circle). These samples are then accumulated into orientation histograms summarizing the contents over 4×4 subregions, as shown on the right, with the length of each arrow corresponding to the sum of the gradient magnitudes near that direction within the region. The figure shows a 2×2 descriptor array computed from an 8×8 set of samples, whereas the experiments in this paper use 4×4 descriptors computed from a 16×16 sample array.

therefore having a $4\times4\times8$=128 element feature vector for each keypoint.

E. Keypoint matching

Matching between two images I_1 and I_2 is performed by comparing each local extrema based on the associated descriptors. Given a feature point p_{11} in I_1, its closest point p_{21}, second closest point p_{22}, and their Euclidean distances d_1 and d_2 are calculated from feature points in I_2. If the ratio d_1/d_2 is sufficiently small, then points p_{11} and p_{21} are considered to match. Then, the matching score between two images can be decided based on the number of matched points. According to [7], we have chosen a threshold of 0.76 for the ratio d_1/d_2.

F. Trimming of false matches

The keypoint matching procedure described may generate some erroneous matching points. We have removed spurious matching points using geometric constraints [10]. We limit typical geometric variations to small rotations and displacements. Therefore, if we place two iris images side by side and draw matching lines as shown in Figure 5 (top), true matches must appear as parallel lines with similar lengths. According to this observation, we compute the predominant orientation θ_P and length ℓ_P of the matching, and keep the matching pairs whose orientation θ and length ℓ are within predefined tolerances ε_θ and ε_ℓ, so that $|\theta-\theta_P|<\varepsilon_\theta$ and $|\ell-\ell_P|<\varepsilon_\ell$. The result of this procedure is shown in Figure 5 (bottom).

III. EXPERIMENTAL FRAMEWORK

A. Database and protocol

For the experiments in this paper, we use the BioSec baseline database [11]. It consists of 200 individuals acquired in two acquisition sessions, separated typically by one to four weeks. A total of four iris images of each eye, changing eyes between consecutive acquisitions, are acquired in each session. The total number of iris images is therefore: 200 individuals × 2 sessions × 2 eyes × 4 iris = 3,200 iris images. We consider each eye as a different user, thus having 400 users. Glasses were removed for the acquisition, while the use of contact lenses was allowed. The database have been acquired with the LG Iris Access 3000 sensor, with an image size of 640 pixels width and 480 pixels height. Some iris examples are shown in Figure 6.

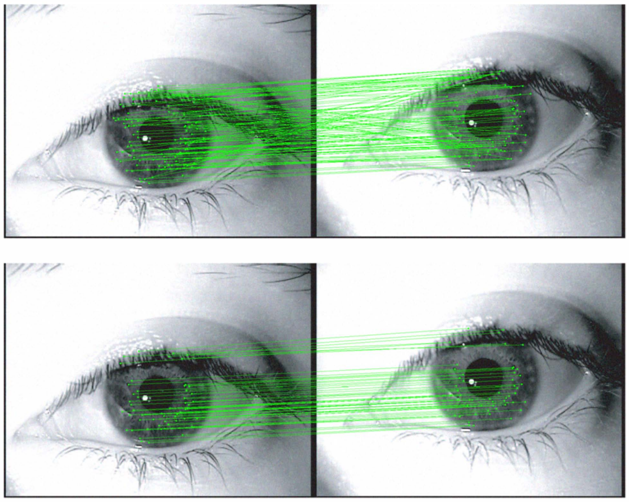


Fig. 5. Matching of two iris images using SIFT operators without and with trimming of false matches using geometrical constraints (top and bottom, respectively). Trimming of false matches is done by removing matching pairs whose orientation and length differ substantially from the predominant orientation and length computed from all the matching pairs.

The 200 subjects included in BioSec Baseline are further divided into [11]: $i)$ the *development set*, including the first 25 and the last 25 individuals of the corpus, totaling 50 individuals; and $ii)$ the *test set*, including the remaining 150 individuals. The development set is used to tune the parameters of the verification system and of the fusion experiments done in this paper (indicated later in this Section). No training of parameters is done on the test set. The following matchings are defined in each set: $a)$ genuine matchings: the 4 samples in the first session to the 4 samples in the second session; and $b)$ impostor matchings: the 4 samples in the first session to 1 sample in the second session of the remaining users. With the development set, this results in 50 individuals $\times$ 2 eyes $\times$ 4 templates $\times$ 4 test images $=1,600$ genuine scores, and 50 individuals $\times$ 2 eyes $\times$ 4 templates $\times$ 49 test images $=19,600$ impostor scores. Similarly, for the test set we have 150 individuals $\times$ 2 eyes $\times$ 4 templates $\times$ 4 test images $=4,800$ genuine scores, and 150 individuals $\times$ 2 eyes $\times$ 4 templates $\times$ 149 test images $=178,800$ impostor scores.

We have automatically segmented all the iris images using circular Hough transform in order to detect the iris and pupil boundaries, which are modeled as two concentric circles [4]. Then, automatically segmented images have been visually inspected to manually correct images not well segmented. With this procedure, we obtain a correct segmentation of the 100% of the database. The objective is avoid bias in the matching performance due to incorrectly segmented images.

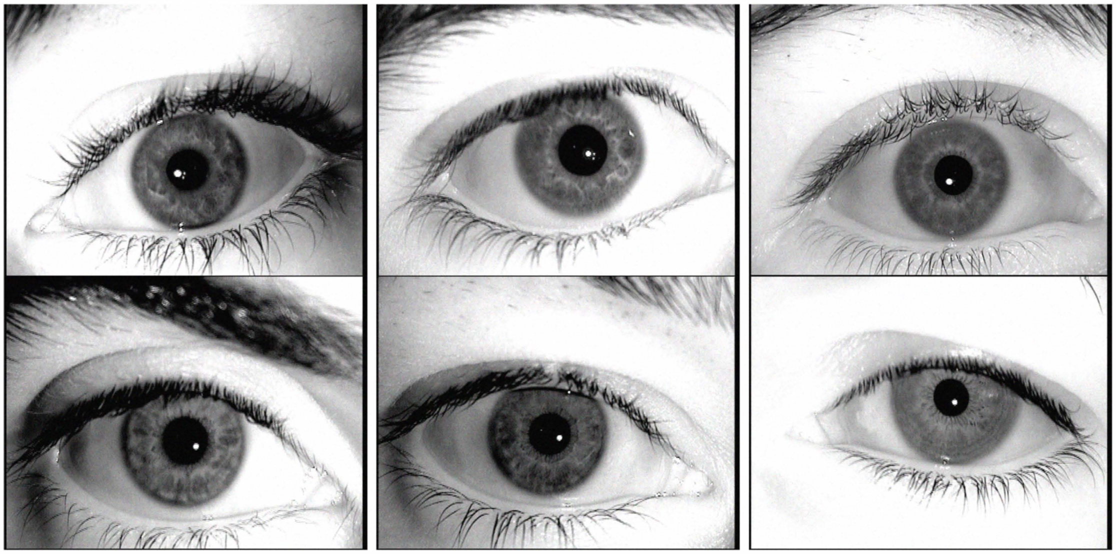


Fig. 6. Iris examples from the BioSec database.

We then construct a binary mask that includes only the iris region and use it to discard SIFT keypoints being detected outside the mask. An example of segmented images together with the detected SIFT keypoints can be seen in Figure 7. Since eyelash and eyelid occlusion is not very prominent in our database, no technique was implemented to detect eyelashes or eyelids.

B. Baseline iris matcher

In order to compare the performance of the proposed iris recognition system based on SIFT features, we use as baseline iris matcher the freely available[1] iris recognition system developed by Libor Masek [12], [13], which is based on transformation to polar coordinates and Log-Gabor wavelets.

This system performs a normalization of the segmented iris region by using a technique based on Daugman's rubber sheet model [4]. The centre of the pupil is considered as the reference point, and radial vectors pass through the iris region. Since the pupil can be non-concentric to the iris, a remapping formula for rescale points depending on the angle around the circle is used. Normalization produces a 2D array with horizontal dimensions of angular resolution and vertical dimensions of radial resolution. This normalization step is as shown in Figure 1.

Feature encoding is implemented by convolving the normalized iris pattern with 1D Log-Gabor wavelets. The 2D normalized pattern is broken up into a number of 1D signals, and then these 1D signals are convolved with 1D Gabor wavelets. The rows of the 2D normalized pattern are taken as the 1D signal, each row corresponds to a circular ring on the iris region. It uses the angular direction since maximum independence occurs in this direction [12].

The output of filtering is then phase quantized to four levels using the Daugman method [4], with each filtering producing two bits of data. The output of phase quantization is a grey code, so that when going from one quadrant to another, only 1 bit changes. This will minimize the number of bits disagreeing, if say two intra-class patterns are slightly misaligned and thus will provide more accurate recognition [12]. The encoding process produces a bitwise template containing a number of bits of information.

For matching, the Hamming distance (HD) is chosen as a metric for recognition, since bitwise comparisons are necessary. In order to account for rotational inconsistencies, when the Hamming distance of two templates is calculated, one template is shifted left and right bitwise and a number of Hamming distance values is calculated from successive shifts [4]. This method corrects for misalignments in the normalized iris pattern caused by rotational differences during imaging. From the calculated distance values, the lowest one is taken.

C. Results

First, the SIFT matcher is optimized in terms of its different parameters. The experimental parameters to be set are: the scale factor of the Gaussian function σ=1.6; the number of scales s=3; the threshold D excluding low contrast points; the threshold r excluding edge points (r=10); the threshold of the ratio d_1/d_2 (set to 0.76) and the tolerances ε_θ and ε_ℓ for trimming of false matches. The indicated values of the parameters have been extracted from Lowe [7]. We have noted however that the threshold D indicated in [7] discards too many SIFT keypoints of the iris region (D=0.03 when pixel values are in the range [0,1]). Thus, together with ε_θ and ε_ℓ, we have decided to find an optimal value also for D.

Figure 8 shows the verification performance of our SIFT implementation on the development set in terms of EER (%) as we vary ε_θ and ε_ℓ when D=0.25/255, D=0.5/255 and

[1] The source code can be freely downloaded from www.csse.uwa.edu.au/˜pk/studentprojects/libor/sourcecode.html

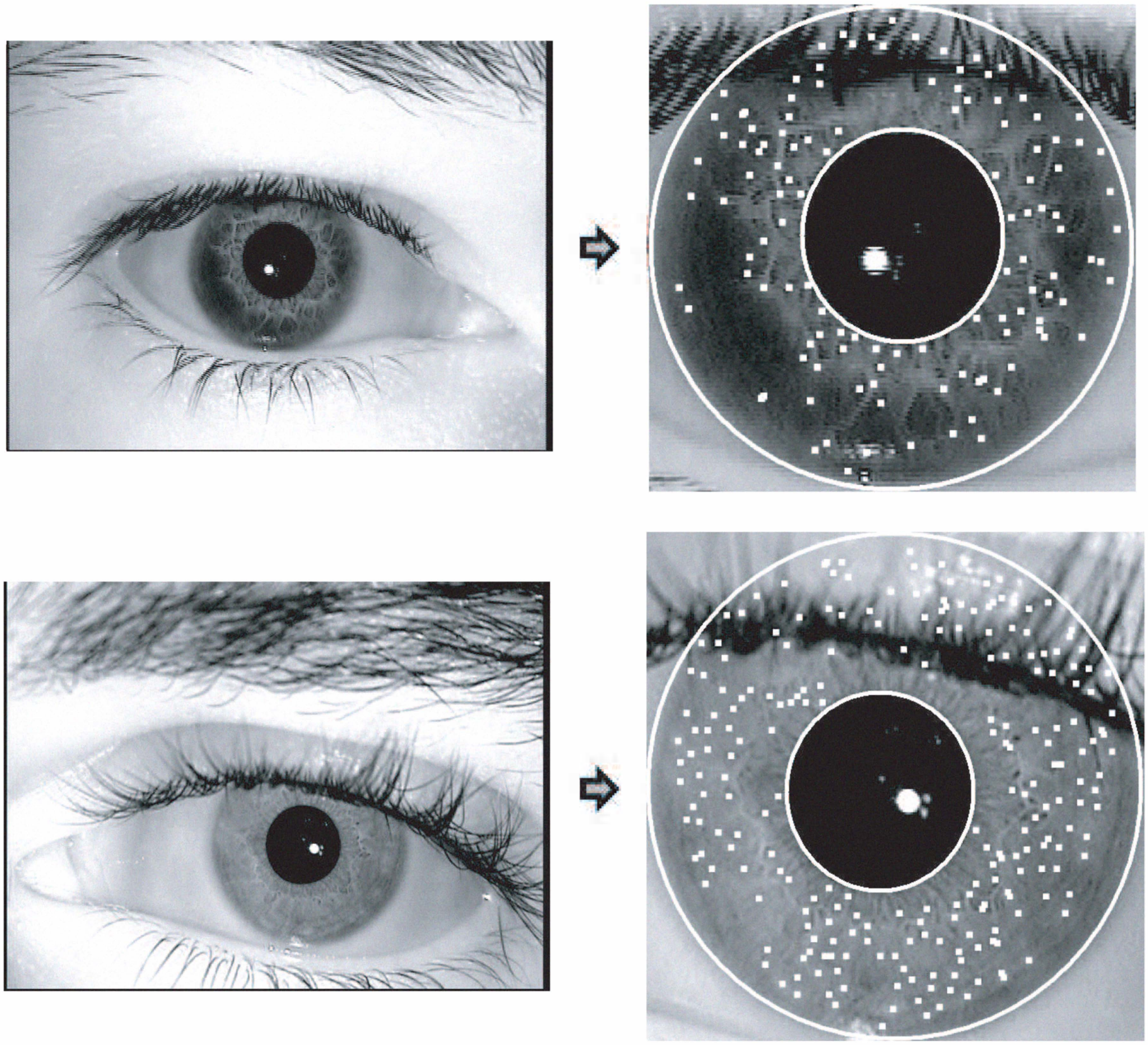


Fig. 7. Example of segmented images together with their detected SIFT keypoints.

D=0.75/255. The optimal combination of parameters in these three cases (i.e. those that results in the lowest EER) are also summarized in Table I, together with the case where no trimming of false matches is carried out. We observe that by trimming out false matches using geometric constraints, the EER is reduced to the fourth part.

Based on the results of Figure 8 and Table I, the best combination of parameters is therefore D=0.25/255, ε_θ=18 and ε_ℓ=14. Figure 9 depicts the performance of the SIFT matcher for this case. We observe that the optimal value of D in our SIFT implementation, D=0.25/255$\simeq$0.00098, is much lower than 0.03 (as recommended in [7]). Concerning the values of the tolerances ε_θ and ε_ℓ, it can be seen in Figure 8 that the EER monotonically decreases as the two tolerances are increased until a minimum in the EER is reached (the exact values of ε_θ and ε_ℓ at the minimum are indicated in Table I). Once this minimum is reached, the EER is slightly increased again with the tolerances.

We now compare the performance of our SIFT implementation with the baseline iris matcher of Section III-B. Figure 10 comparatively shows the performance of the two matchers using DET curves, both on the development and on the test set. We also have performed a fusion of the SIFT and baseline matchers using sum rule with tanh normalization [15]:

$$s' = \frac{1}{2}\left\{\tanh\left(0.01\left(\frac{s-\mu_s}{\sigma_s}\right)\right)+1\right\} \qquad (3)$$

where s is the raw similarity score, s' denotes the normalized similarity score, and μ_s and σ_s are respectively the estimated mean and standard deviation of the genuine score distribution. Table II summarizes the Equal Error Rates (EER) computed from Figure 10. We observe that the fusion of the two matchers results in better performance than either of the two matchers,

IV. CONCLUSIONS AND FUTURE WORK

In this paper, we have proposed the use of the SIFT operator for iris feature extraction and matching. There have been a few studies using SIFT for face [8], [9] and fingerprint [10] recognition, and some recent studies also for iris [5]. In this work, we contribute with the analysis of the influence of

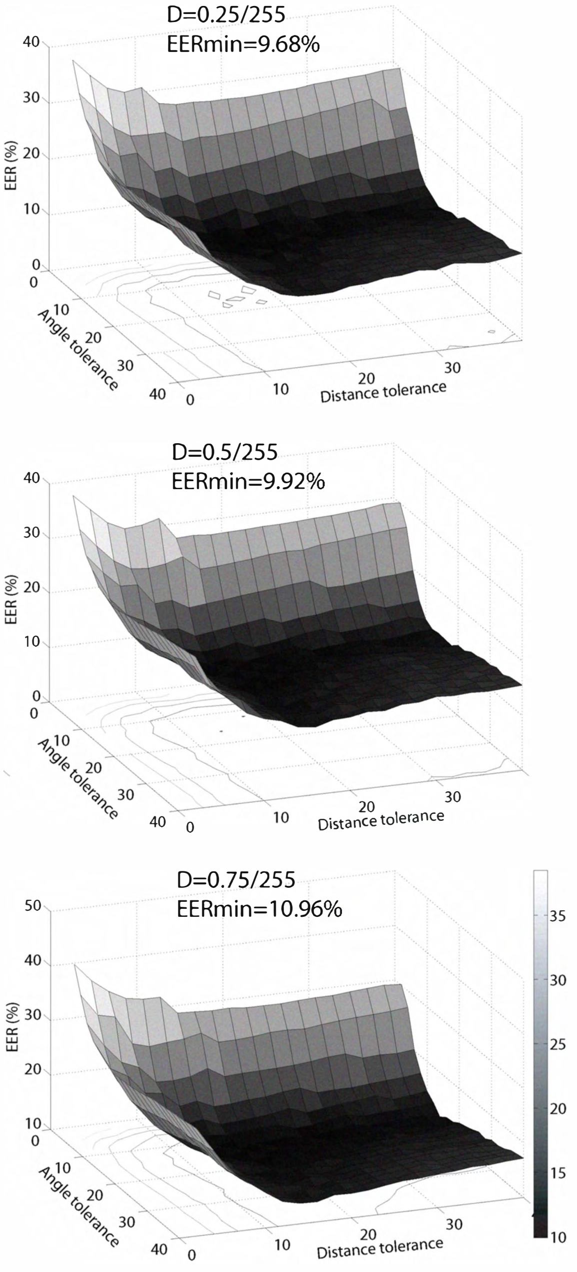


Fig. 8. Development set. Verification results of the SIFT matcher in terms of EER (%) depending on the threshold D and the tolerances of angle (ε_θ) and distance (ε_ℓ).

different SIFT parameters on the verification performance, including trimming of false matches with geometric constraints, as proposed in [10] for the case of fingerprints. Although the performance of our implementation is below popular matching approaches based on transformation to polar coordinates and Log-Gabor wavelets, we also show that their fusion provides a performance improvement of 24% in the EER. This is because the sources of information used in the two matchers are different, providing complementary sources of information.

D	ε_θ	ε_ℓ	EER
0.25	-	-	36.85%
0.25	**18**	**14**	**9.68%**
0.5	14	16	9.92%
0.75	18	14	10.96%
1	16	14	14.03%

TABLE I

DEVELOPMENT SET - SIFT MATCHER. OPTIMAL COMBINATIONS OF THE PARAMETERS D AND TOLERANCES OF ANGLE (ε_θ) AND DISTANCE (ε_ℓ). THE COMBINATION RESULTING IN THE LOWEST EER IS MARKED IN BOLD. THE FIRST ROW INDICATES THE CASE WHERE NO TRIMMING OF FALSE MATCHES IS CARRIED OUT.

	SIFT	Baseline	Fusion
Development set	9.68%	4.64%	-
Test set	11.52%	3.89%	2.96%

TABLE II

EER OF SIFT, BASELINE AND FUSION MATCHERS.

Future work will be focused on the improvement of the SIFT matcher by detecting eyelids, eyelashes and specular reflections [6], thus discarding SIFT keypoints computed in these regions. We are also working on the inclusion of local iris quality measures [16] to account for the reliability of extracted SIFT points, so if the quality is high for two matched points, they will contribute more to the computation of the matching score.

Current iris recognition systems based on accurate segmentation and transformation to polar coordinates rely on cooperative data, where the irises have centered gaze, little eyelashes or eyelids occlusion, and illumination is fairly constant [5]. The SIFT-based method does not require polar transformation or highly accurate segmentation, and it is invariant to illumination, scale, rotation and affine transformations [7]. This makes the SIFT approach feasible for biometric recognition of distant and moving people, e.g. the “Iris on the Move” project [14], where a person is recognized while walking at normal speed through an access control point such as those common at airports. Currently this is one of the research hottest topics within the international biometric community [17], which drastically reduces the need of user’s cooperation, and it will be another important source of future work.

V. ACKNOWLEDGMENTS

This work has been supported by Spanish MCYT TEC2006-13141-C03-03 project. Author F. A.-F. is supported by a Juan de la Cierva Fellowship from the Spanish MICINN.

REFERENCES

[1] A.K. Jain, A. Ross, and S. Pankanti, “Biometrics: A tool for information security,” *IEEE Trans. on Information Forensics and Security*, vol. 1, pp. 125–143, 2006.

[2] A. Jain, R. Bolle, S. Pankanti, Eds., *Biometrics - Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

[3] Donald M. Monro, Soumyadip Rakshit, and Dexin Zhang, “DCT-Based iris recognition,” *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 586–595, April 2007.

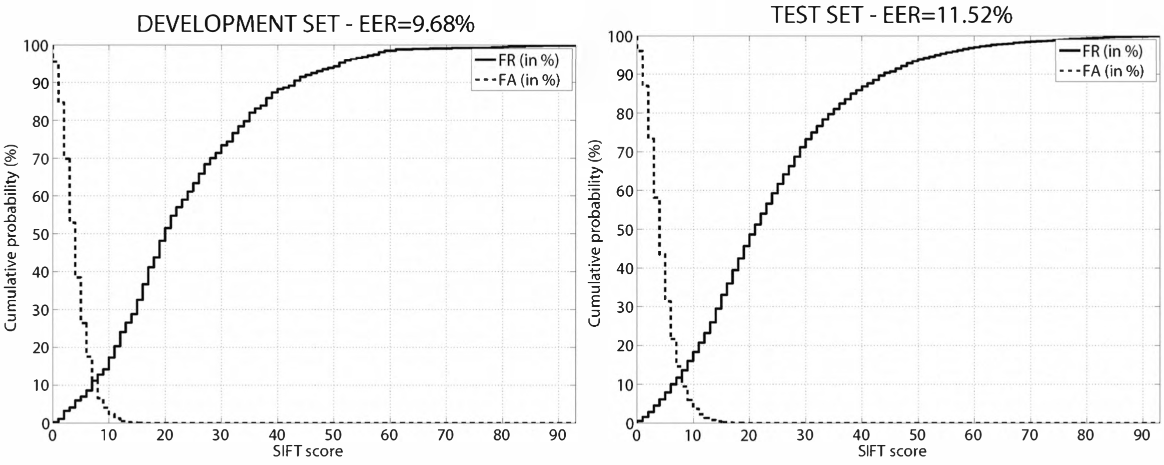


Fig. 9. Performance of the SIFT matcher (FR=False Rejection, FA=False Acceptance).

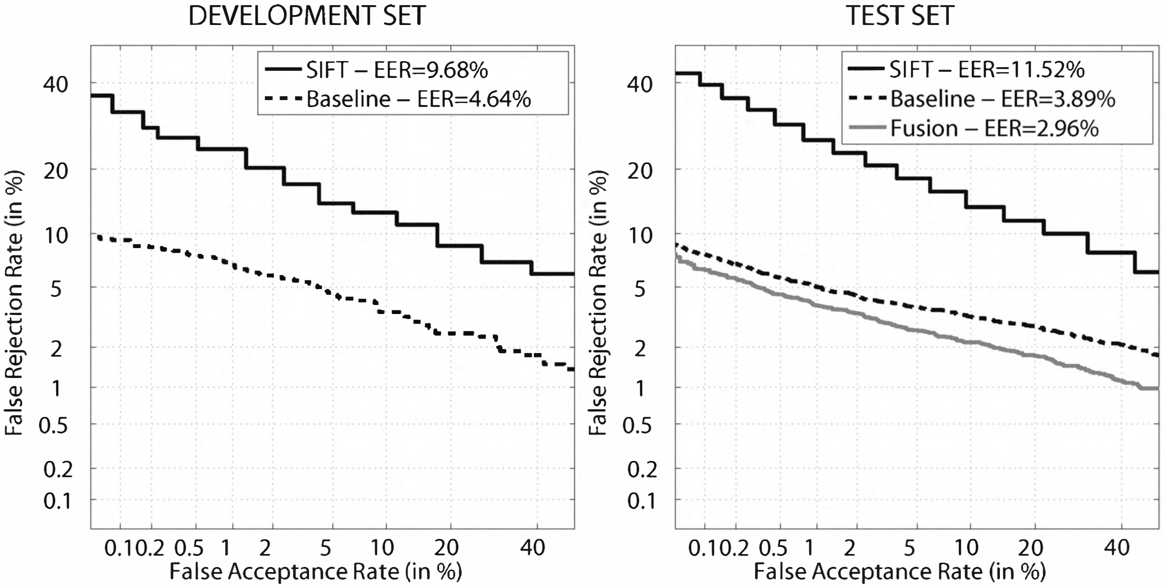


Fig. 10. Performance of the SIFT and the baseline matchers and their fusion results.

[4] John Daugman, "How iris recognition works," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, pp. 21–30, 2004.

[5] Craig Belcher and Yingzi Du, "Region-based SIFT approach to iris recognition," *Optics and Lasers in Engineering*, vol. 47, no. 1, pp. 139–147, 2009.

[6] K.W. Bowyer, K. Hollingsworth, and P.J. Flynn, "Image understanding for iris biometrics: a survey," *Computer Vision and Image Understanding*, vol. 110, pp. 281–307, 2008.

[7] D. Lowe, "Distinctive image features from scale-invariant key points," *Intl Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.

[8] D.R. Kisku, A. Rattani, E. Grosso, and M. Tistarelli, "Face identification by SIFT-based complete graph topology," *Proc. IEEE AUTOID*, pp. 63–68, 2007.

[9] Jun Luo, Yong Ma, Erina Takikawa, Shihong Lao, Masato Kawade, and Bao-Liang Lu, "Person-specific SIFT features for face recognition," *Proc. IEEE ICASSP*, vol. 2, pp. 593–596, 2007.

[10] U. Park, S. Pankanti, and A. K. Jain, "Fingerprint verification using SIFT features," *Defense and Security Symposium, Biometric Technologies for Human Identification, BTHI, Proc. SPIE*, 2008.

[11] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, J. Gonzalez-Rodriguez, "BioSec baseline corpus: A multimodal biometric database," *Pattern Recognition*, vol. 40, no. 4, pp. 1389–1392, 2007.

[12] Libor Masek, *Recognition of human iris patterns for biometric identification*, Ph.D. thesis, Technical Report, The school of Computer Science and Software Engineering, The University of Western Australia, 2003.

[13] L. Masek and P. Kovesi, "Matlab source code for a biometric identification system based on iris patterns," *The School of Computer Science and Software Engineering, The University of Western Australia*, 2003.

[14] J.R. Matey, O. Naroditsky, K. Hanna, R. Kolczynski, D. LoIacono, S. Mangru, M. Tinker, T. Zappia, and W.Y. Zhao, "Iris on the move: acquisition of images for iris recognition in less constrained environments," *Proc. IEEE*, vol. 94, no. 11, pp. 19361946, 2006.

[15] A.K. Jain, K. Nandakumar, and A. Ross, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270–2285, December 2005.

[16] Y. Chen, S. Dass, and A. Jain, "Localized iris image quality using 2-D wavelets," *Proc. International Conference on Biometrics, ICB*, vol. Springer LNCS-3832, pp. 373–381, 2006.

[17] NIST MBGC, *NIST Multiple Biometric Grand Challenge - http://face.nist.gov/mbgc*, 2007.