UNIVERSIDAD AUTONOMA DE MADRID

ESCUELA POLITECNICA SUPERIOR

PROYECTO FIN DE CARRERA

SISTEMA DE DETECCIÓN DE VIDA VÍA SOFTWARE EN IMÁGENES DE IRIS UTILIZANDO CRITERIOS DE CALIDAD

Jaime Ortiz López

OCTUBRE 2011

SISTEMA DE DETECCIÓN DE VIDA VÍA SOFTWARE EN IMÁGENES DE IRIS UTILIZANDO CRITERIOS DE CALIDAD

AUTOR: Jaime Ortiz López
TUTOR: Javier Galbally Herrero

Grupo de Área de Tratamiento de Voz y Señal (ATVS)
Dpto. de Tecnología Electrónica y Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Septiembre de 2011

Resumen:

En este proyecto se estudia, implementa y evalúa un sistema automático de detección de vida en imágenes usando medidas de calidad. Se trata de un sistema capaz de detectar intentos de intrusión previamente a la identificación o verificación del usuario en los sistemas biométricos de autentificación de iris mediante el análisis de las imágenes capturadas por el sensor.

El proyecto surge ante la necesidad de búsqueda de contramedidas a ataques a sistemas automáticos de autentificación biométricos mediante uso de falsificaciones de imágenes reales de iris.

Tras una introducción a la biometría, estudio del iris, del estado del arte en contramedidas y ataques y de métodos de detección de vida, se buscó una parametrización con suficiente nivel discriminativo entre imágenes reales y falsas de iris. Para ello se implementaron una serie de factores de calidad propuestos en la literatura y se propusieron nuevas medidas modificando las dadas por otros investigadores.

En la parte de experimentos, se realizaron 3 fases bien diferenciadas:

i) Se observó el comportamiento de los conjuntos de imágenes (original y falso) en relación a cada una de las medidas implementadas y posteriormente se dividieron las bases de datos para realizar la segunda y tercera fase de los experimentos (entrenamiento y test).
ii) Prueba de la capacidad de detección de las 22 medidas implementadas y subconjuntos de las mismas utilizando los datos de entrenamiento.
iii) Obtención de los resultados definitivos del sistema, observando la capacidad de detección de los mejores subconjuntos en la fase ii) utilizando para estos resultados los datos de test.

Por último se evaluó las posibles diferencias entre los resultados en las fases de entrenamiento y de test y se utilizan estos resultados para presentar conclusiones y proponer líneas de trabajo futuro.

Este proyecto aporta una herramienta de detección de falsos iris con una tasa de acierto muy alta para la base de datos utilizadas. Además la investigación para el proyecto ha dado lugar al envío de 2 artículos a congresos internacionales.

Palabras Clave:

Biometría, procesamiento de imágenes, ataques a sistemas biométricos, reconocimiento de iris, contramedidas biométricas, sistemas de detección de vida, medidas de calidad.

Abstract:

In this M.Sc. Thesis, we study, implement and test an iris liveness detection system. This is an anti-spoofing system which detects possible attacks before the identification or verification process applying image processing techniques to the sample taken by the sensor.

The idea of the project comes from the need to find countermeasures to direct attacks to biometric authentication systems using forgery images of real eyes.

After a review of the state of the art of biometrics, and more specially of iris-liveness detection systems, we select and implement the best features proposed with enough discriminative power, and we propose new features using adapted from different state-of-the-art works.

In the experimental section, three different stages may be differentiated:

i) We analyzed the behavior of the image sets (original and fake) for each of the 22 implemented features and later we divided the data base to carry out the second and the third stages (train and test).
ii) We assessed the liveness detection capability of the set of 22 features, also we studied different subsets using the training subset.
iii) We got the final results evaluating the liveness detection capability of the best subsets found in ii) using for this stage the test subset.

Finally we evaluate the possible differences between train and test results, then we use the results to present conclusions and based on them, some future direction to improve the implemented system.

This M.Sc. Thesis, presents a liveness detection toolkit on iris images with a very high classification accuracy in the data bases used in the investigation. Even this research work has led us to submit two papers to international peer reviewed conferences.

Key Words:

Biometrics, image processing, attacks to biometric systems, iris recognition, biometric countermeasures, liveness detection systems, quality features.

Agradecimientos:

Quiero agradecer en primer lugar a mi ponente, Javier Ortega, la oportunidad que me ha brindado de colaborar con el ATVS y su apoyo para realizar mi Proyecto de Fin de Carrera.

En segundo lugar me gustaría también agradecer a mi tutor, Javier Galbally, me ha guiado, ayudado y animado durante este proyecto.

Como no podía ser de otra forma mi tercer agradecimiento es para Julián Fierrez ya que él fue mi puerta a este magnífico grupo de investigación y de personas.

En cuarto lugar, vienen todos los miembros del C-109 becarios, no-becarios, babies, doctorandos y proyectandos. Habéis, tanto directa como indirectamente, hecho que mi paso por el grupo sea una experiencia muy agradable y que no olvidaré. Gracias Pedro por tu infinita paciencia para ayudarme en mis peores momentos, gracias Marta por esos cables, ya que sin ellos no hubiese podido llegar aquí. No olvidaré los constantes intentos de tomar café a Miriam, María, Javi G, Iñaki, Javi F, Laura y por supuesto a mi súper compañero de paddle, Rubén pero ya sabéis soy una persona muy ocupada.

Faltan mis compis de línea Eva, Eugenio y Álvaro: habéis aguantado de forma excepcional mis idas de pinza y mis infinitas historias además de ayudarme en temas del proyecto.

El grupo ATVS no son sólo estas personas que he nombrado, no me olvido de gente como Joaquín González o Doroteo Torre, profesores mío en dos asignaturas y en parte culpables de mi elección del grupo de investigación para mi proyecto.

Un gran profesor y si cabe mejor persona me dejo en el tintero, Daniel Ramos, me has enseñado una forma de ver la vida diferente de forma desenfada y a apreciar lo que realmente vale la pena, nunca olvidaré nuestras charlas elípticas.

De maestro a aprendiz que un día será un grande en todos los aspectos, Sr. Sergio Pérez, el tiempo lo ha demostrado y cualquiera puede darme la razón. Pulcro, currante, impecable y perfeccionista, así es él tanto en el trabajo como en la amistad, alguien que hay que mantener siempre cerca y cuidar la amistad, pese a que en eso yo sea un caos.

Toca el turno de mis compañeros de rutina, cierto es que nunca me he visto no encajar en ningún grupo hasta que Sergio, Jorge, David, Javi, Laura, Ajito…me abrieron sus brazos yo formé parte de algo.

La frase *"cabalgamos juntos, morimos juntos, rebeldes para siempre"* además de ser de una película tiene un significado especial para mí y espero que para Ángel también sea especial.

Para finalizar, toca el turno de mi núcleo familiar: Javi, enano y mis padres con los que no siempre han ido las cosas bien, aunque siempre han estado allí para ayudarme y

empujarme en los momentos buenos y en los no tan buenos para poder resurgir como el fénix. Papá y Mamá, vosotros sois los culpables de que hoy esté presentando mi Proyecto de Fin de Carrera y os estaré eternamente agradecido.

Papá tú me diste la idea de hacer una ingeniería y me has enseñado y has aportado tu fuerza de voluntad y cuando más perdido estaba tendiste tu mano y me ayudaste a despegar de nuevo. Hace 3 años me enviaste un email que me cambió, *"querer es poder""¡vamos, juntos, a buscarlo!"* (hoy me sigo emocionando al leerlo) a ti te digo hoy: " B1…, rotate…, positive!...landing gear up!".

Mamá tú has estado ahí día a día deseándome suerte en cada examen y sufriendo conmigo cada día de universidad, mis estreses, mis lloros y mis alegrías. Me has enseñado y me has escuchado siempre que lo he necesitado y siempre me has dicho lo mejor para mí eres una gran consejera y mejor madre .

MUCHAS GRACIAS

Jaime Ortiz López

Septiembre 2011

“Necesariamente vence siempre el entusiasta al apático. No es la fuerza del brazo, ni la virtud de las armas, sino la fuerza del alma la que alcanza la victoria. ”

Johann Gottlieb Fichte

A mis padres

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 Tecnología de Electrónica y Comunicaciones, Escuela Politécnica Superior, Universidad Autónoma de Madrid.

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

1. INTRODUCCIÓN

1.1. MOTIVACIÓN

El aumento del uso de las tecnologías de la información y el incremento de los requerimientos de seguridad han conllevado un **rápido desarrollo de sistemas inteligentes de identificación personal basados en técnicas biométricas**. Las técnicas biométricas usan características o comportamientos fisiológicos propios de cada individuo para identificarlo.

Una de las técnicas utilizadas es el reconocimiento del iris, una técnica relativamente reciente en el ámbito de la identificación personal, considerada como uno de los medios más fiables dentro de la biometría**.**

Actualmente el uso de técnicas de reconocimiento y autenticación mediante iris está cobrando **gran relevancia,** ya que supone una **forma segura y efectiva de identificación de personas**. La principal ventaja de los sistemas de reconocimiento de iris consiste en que son **difícilmente falseables.** No obstante a la vez que las técnicas de detección y autentificación **mejoran**, también lo hacen **las técnicas de ataque a los sistemas biométricos.**

Existen dos tipos de ataques: **directos e indirectos.** Los primeros son aquellos llevados a cabo directamente sobre el sensor y los segundos aquellos que atacan alguna parte interna del sistema, siendo necesario para ello tener algún tipo de información específica sobre la aplicación (codificación de plantillas, información almacenada, etc.).

En el campo del iris, los principales intentos por falsear al usuario mediante ataques directos al sensor autorizado son el uso de lentillas, de fotografías del iris del usuario, uso de vídeos grabados e incluso haciendo uso de imágenes de iris generadas sintéticamente [1], [2].

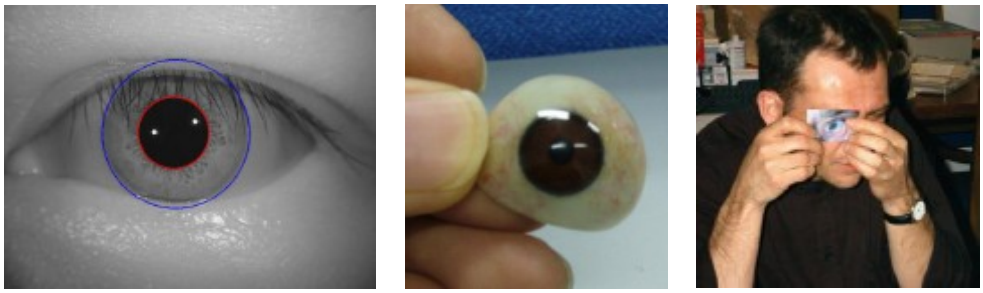
Los principales esfuerzos para contrarrestar este tipo de ataques han ido dirigidos a desarrollar **algoritmos de detección de vida.** Estas técnicas intentan distinguir entre iris reales y sintéticos utilizando medidas vía hardware (p.e. método challenge-response [3] [4]) o a través del tratamiento software de la propia muestra de entrada [5]. **Los algoritmos de software** tienen la **ventaja** de no introducir nuevos dispositivos en el sensor, con el consiguiente **abaratamiento y simplificación del sistema.**

Hasta el momento la mayor parte de los **métodos de detección de vida** se basan en perspectivas **hardware**, lo que hacen que el sistema de identificación se vuelva más invasivo y caro.

La motivación del proyecto surge como búsqueda de una alternativa a las técnicas hardware de detección de vida en iris para contrarrestar los ataques directos, de

forma que se consiga aumentar la conveniencia para el usuario de los sistemas automáticos de reconocimiento de iris **sin disminuir su nivel de seguridad ni eficacia.**

Como precedente, se puede tomar el estudio sobre la detección de vida en huella dactilar vía software usando factores de calidad [8] y los numerosos estudios sobre identificación de iris [9,11,37,44]**.**



(a) **(b)** **(c)**

Figura 1. Iris, pupila y esclera en un ojo (a), ojo sintético (b) e intento de suplantación (c).

1.2. OBJETIVOS

El objetivo del proyecto es desarrollar un **sistema software de detección de vida** a través de la utilización de una parametrización basada en criterios de **medida de calidad** del iris.

Para ello se ha estudiado la relación de los **criterios de calidad** en las imágenes de iris con la existencia de vida en el iris del que se ha tomado la imagen comprobando si son aptos para desarrollar un sistema software de detección de vida que ayude a aumentar la seguridad de los sistemas de reconocimiento automático basado en este rasgo frente a ataques directos.

1.3. METODOLOGÍA Y PLAN DE TRABAJO

Para la obtención de los objetivos se han seguido los siguientes pasos:

- Familiarización con las bases de datos de Iris del grupo ATVS, así como con las herramientas de procesamiento de bases de datos necesarias.
- Familiarización con los principales rasgos discriminativos del iris.
- Implementación de los diferentes indicadores de calidad sobre imágenes de iris, reconocidas y publicadas en diversos artículos internacionales.
- Enfrentar las bases de datos a estos factores de calidad y obtener sus medidas.
- Búsqueda con el conjunto de entrenamiento mediante un clasificador y un algoritmo de selección de características la combinación óptima de características que permitan un mínimo error al distinguir entre original o falso.
- Enfrentar las combinaciones halladas con las imágenes de entrenamiento a las imágenes de testeo y obtener resultados finales.
- Extracción de conclusiones.
- Publicación de resultados y conclusiones.

1.4. ESTRUCTURA

En el capítulo 2 del proyecto se realiza una introducción a la biometría, comenzando por dar unas pequeñas pinceladas sobre diferentes rasgos biométricos y sus características (secciones 2.1 y 2.2) . Posteriormente se presentan los sistemas biométricos y los sistemas automáticos de reconocimiento (2.3 y 2.4).

El capítulo 3 se centra en los sistemas de reconocimiento de iris, partiendo de la evolución de estos sistemas en el tiempo, incidiendo en el ojo y su anatomía y posteriormente

mostrando el estado del arte en el campo de la adquisición y reconocimiento de imágenes de iris.

En el capítulo 4 se hace un resumen sobre los principales métodos de ataque actuales a los sistemas biométricos centrándose en los ataques a sistemas de iris. La siguiente parte del capítulo se centra en las principales contramedidas a estos ataques y en especial en la disciplina de la detección de vida dando ejemplos actuales de métodos implementados.

El capítulo 5 describe el sistema de detección de vida implementado, su estructura general y presentación de cada una de sus partes.

La presentación de la base de datos y el protocolo experimental se hace en el capítulo 6 y en el siguiente capítulo presentamos los resultados obtenidos en la investigación, para en el capítulo 8 presentar las conclusiones y trabajo futuro.

1.5. CONTRIBUCIONES CIENTÍFICAS

Parte del trabajo recogido en esta memoria ha sido realizado con la financiación de una **Beca de Colaboración del MEC**. Entre las tareas más representativas han estado:

- Estudio e implementación de 22 factores de calidad utilizados para la investigación.
- Adaptación del código de selección de características (SFFS) en función del error de clasificación de los 22 parámetros implementados.
- Adaptación del algoritmo generado para la predicción de vulnerabilidades en imágenes de iris (a ser fácilmente plagiadas o no) con parámetros de calidad (ANEXO I).

Este trabajo de investigación ha dado lugar a dos artículos en congresos internacionales con revisión, (anexo I del proyecto):

- J.Ortiz-Lopez, J.Galbally, J.Fierrez, J.Ortega-García "Predicting Iris Vulnerability to Direct Attacks Based on Quality Related Features" In: Int.Carnahan Conf. on Security Technology (ICCST), Barcelona 2011 (accepted).

- J.,Galbally, J.Ortiz-Lopez, J.Fierrez and J.Ortega-García "Iris Liveness Detection Based on Quality Related Features" In: Int. Conference on Biometrics (ICB) New Delhi 2012(submitted)

2. INTRODUCCIÓN A LA BIOMETRÍA

Biometría: "Estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos".

Según la definición, podríamos afirmar que la biometría es la ciencia que nos permite utilizar nuestros rasgos físicos y conductuales como un "identificador" o una "llave" reconocible.

Definiremos pues esos identificadores o llaves como rasgos biométricos y serán utilizados para reconocimiento, identificación y verificación de identidad.

Como ejemplo de identificador podríamos hablar del rasgo más reconocido probablemente por la sociedad debido a la difusión de series de investigación criminal, la huella dactilar.

Las huellas dactilares son un buen ejemplo de identificación ya que ayudan al reconocimiento de personas que han estado o están en determinados lugares, al igual que lo hace el ADN.

Para poner un ejemplo en cuanto al símil del rasgo biométrico como una llave, basta con interpretarlo como un código intrínseco a nuestro organismo (siempre, salvo amputaciones o accidentes, estará presente) y que nos permite acceder a sistemas y lugares preparados para solo dejar acceso a determinados códigos (o individuos).

En cuanto al reconocimiento biométrico, presenta una gran ventaja con respecto a los demás tipos de sistemas de seguridad (llave, pin, contraseña…) debido a que este no puede ser olvidado, robado o perdido, ya que es intrínseco al individuo.

En este capítulo se hablará de las características de los rasgos biométricos, posteriormente se habla de los principales rasgos biométricos y sus características más importantes para su utilización en los sistemas de autentificación y reconocimiento. En el tercer apartado se habla del los sistemas biométricos y por último el apartado 2.4 hablamos de los sistemas automáticos de reconocimiento basados en estos rasgos.

La finalidad de este capítulo es la presentación de los sistemas biométricos en general para posteriormente pasar a indagar más ampliamente en los sistemas automáticos de identificación basados en iris (capítulo 0), en sus vulnerabilidades y contramedidas (capítulo 4).

2.1. CARACTERÍSTICAS DE LOS RASGOS BIOMÉTRICOS

Dentro de la biometría hay muchos campos de estudio que se pueden utilizar para identificar al usuario, podemos realizar una primera división en dos grandes grupos, rasgos morfológicos o anatómicos (p.e. huella, iris, voz, cara...) y rasgos de comportamiento (p.e. firma, escritura, forma de andar…).

Ambos grupos tienen unas características comunes aunque dependiendo de cada rasgo biométrico las tienen en mayor o menor medida:

- **Universalidad:** existencia del rasgo en todos los individuos que tengan que usar el sistema de reconocimiento.
- **Unicidad:** capacidad discriminativa del rasgo (personas distintas deben poseer rasgos diferenciables).
- **Permanencia o estabilidad:** invariancia del rasgo en el tiempo.
- **Mensurabilidad o evaluabilidad:** capacidad para caracterizar el rasgo cuantitativamente, ser medido.
- **Aceptabilidad:** grado de aceptación personal y social.
- **Rendimiento:** precisión y rapidez en la identificación del individuo.
- **Vulnerabilidad:** resistencia a ser eludido o burlado.

Estas son algunas de las características que poseen los rasgos biométricos, las anteriormente presentadas son las que consideramos más importantes.

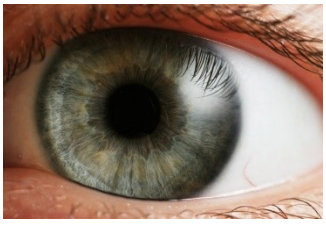
En el siguiente apartado (2.2) se presentan los principales rasgos biométricos utilizados en la actualidad.

2.2. RASGOS BIOMÉTRICOS

Todo rasgo biométrico posee los anteriores atributos mostrados en el apartado 2.1 pero no existe ninguno que sea el mejor de todos ellos.

Cada rasgo biométrico es fuerte en algunos campos, en cambio en otros es débil. Esta característica hará que dependiendo de las necesidades del usuario y el sistema se utilice un rasgo u otro ya que todos tienen sus ventajas y desventajas y por ello resultan muy útiles para algunas aplicaciones pero en cambio ineficaces para otras.

Pasamos pues a detallar brevemente los más utilizados:

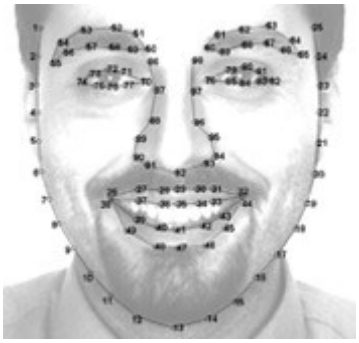


Iris. El iris es muy distintivo para cada uno de los dos ojos del individuo. Aunque su captura requiere un grado de participación por parte del usuario bastante alto, se evoluciona hacia sistemas mucho menos intrusivos que permiten capturar el iris incluso con el usuario en movimiento. En la actualidad se han

desarrollado sistemas que trabajan con cámaras de 2Mpixels lo que permitiría tener un sistema de reconocimiento automático de iris en cualquier ordenador con webcam o incluso en PDAs y smartphones.

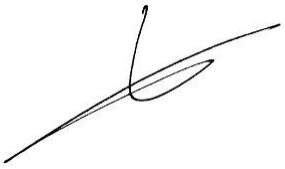
Huella dactilar. Uno de los métodos más conocidos en la sociedad, debido a su uso policial y forense. Una huella consiste en un conjunto de valles y crestas que son capturados al presionar el dedo frente a un sensor o una superficie. Este método es muy barato y muy exacto, pero tiene el inconveniente de su fácil falseabilidad.

Cara. Uno de los rasgos biométricos mas aceptados ya que es el que más usamos los humanos para reconocernos entre nosotros junto a la voz. Para adquirir el rasgo basta con una fotografía, un método nada invasivo. Los principales inconvenientes es la facilidad de falseo y la disminución de rendimiento con los cambios con la edad del usuario, la iluminación, expresiones y la posición con respecto a la cámara.

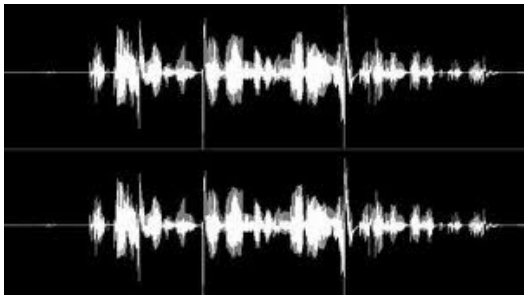


Geometría de la mano. Se trata de la medición de características físicas como la forma de la mano, el tamaño de la palma, la longitud y el ancho de los dedos. Los factores ambientales no suponen un problema, pero la geometría de la mano posee baja distintividad de cada individuo y está sujeto a cambios a lo largo de la vida del usuario.

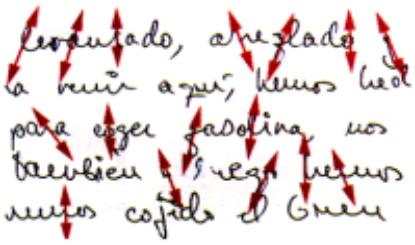
Firma. La forma de firmar de cada persona es característica de cada persona, requiere contacto con una superficie y cooperación del usuario, es un rasgo muy aceptado como método de autentificación, usado para muchas transacciones. La firma varía a lo largo del tiempo en el individuo y además está influenciado por su estado físico y emocional. Existen individuos en los que su firma varia significativamente entre cada realización, lo que hace difícil la identificación.



Voz. Combinación de características físicas y conductuales. Las características físicas del usuario permanecen casi invariantes en el tiempo (fuera del periodo de crecimiento) pero las características de la conducta cambian a lo largo del tiempo y se ven influenciadas por la edad, afecciones médicas o estado de ánimo de la persona. Una de sus desventajas es la facilidad



de suplantación de usuario, pero como ventajas tenemos que es un rasgo biométrico muy aceptado y fácil de capturar.



Escritura. Es uno de los rasgos biométricos del comportamiento, es variable con el tiempo, pero su captura es poco invasiva. Este rasgo al ser tan variable con el tiempo no posee un alto nivel discriminativo como otros métodos como puede ser el iris o las huellas dactilares.

En la tabla 2.1 se puede observar cada uno de los rasgos definidos en este apartado con el grado (cualitativo, **B**ajo, **M**edio o **A**lto) en el que poseen las características definidas en el apartado 2.1.

Rasgo\ Característica	Universalidad	Unicidad	Permanencia	Mensurabilidad	Rendimiento	Aceptabilidad	Vulnerabilidad
Iris	A	A	A	M	A	B	B
Huella dactilar	M	A	A	M	A	M	M
Cara	A	B	M	A	B	A	A
Geometría de la mano	M	M	M	A	M	M	M
Firma	B	B	B	A	B	A	A
Voz	M	B	B	M	B	A	A
Escritura	B	B	B	A	B	A	A

Tabla 1. Comparativa cualitativa de los rasgos biométricos

En el siguiente apartado describiremos la forma de utilizar los rasgos biométricos para integrarlos en sistemas que nos permitan medir sus cualidades y características discriminativas.

2.3. SISTEMAS BIOMÉTRICOS

Un sistema biométrico consiste en un sistema reconocedor de patrones cuyo modo de operación es el siguiente: captura un rasgo biométrico, extracción de un conjunto de características y comparación con uno o varios patrones almacenados en una base de datos para posteriormente tomar la decisión acerca de la identidad del individuo.

2.3.1. APLICACIONES DE LOS SISTEMAS BIOMÉTRICOS

La necesidad de seguridad se ha disparado con el auge de Internet, las compras on-line, las transacciones bancarias vía web o los atentados del 11-S.

La biometría se erige como el futuro de los sistemas de seguridad y su desarrollo en los últimos años ha experimentado un gran crecimiento respecto a otras tecnologías de seguridad. Su eficacia potencial la hacen especialmente interesante en determinadas áreas, en las que ya se empiezan a emplear muchos sistemas biométricos.

Las aplicaciones de los sistemas biométricos se dividen en los siguientes grupos:

- Aplicaciones comerciales: protección de datos electrónicos, red, e-comercio, cajeros automáticos, control de acceso físico…
- Aplicaciones gubernamentales: DNI, carné de conducir, pasaporte, control de fronteras…
- Aplicaciones forenses: identificación de cadáveres, investigación criminal, identificación de terroristas, identificación de parentesco…

2.3.2. PROBLEMAS Y LIMITACIONES DE LOS SISTEMAS BIOMÉTRICOS

A pesar de las evidentes ventajas, los rasgos biométricos de una persona o individuo y su representación varían (unas más que otras) según el método de adquisición, el entorno en el que se realiza la captura y la interacción del usuario con el sistema de adquisición.

Las razones más comunes por las que se producen estas variaciones son:

- Presentación inconsciente: la señal capturada por el sensor depende tanto de las características intrínsecas del rasgo biométrico como de la forma que se presenta dicho rasgo.
- Los rasgos biométricos representan medidas de una característica biológica o de comportamiento y están expuestos a accidentes y heridas que pueden cambiar su estructura de forma permanente, a cambios en su aspecto externo debido a adornos como joyas, maquillaje…

- Captura imperfecta: las condiciones de captura en la práctica no son perfectas y causan variaciones en la señal capturada, diferente iluminación, ruido externo, limitaciones de rendimiento…

Además los sistemas biométricos presentan una serie de problemas aún por resolver, entre ellos:

- Seguridad: no están exentos de ataques externos que puedan comprometer sus niveles de seguridad. Es en este campo conde se enmarca el presente trabajo de investigación como búsqueda de contramedidas a estos ataques (de los cuales se hablará en el capítulo 0).
- Privacidad: algunos rasgos biométricos pueden vulnerar la privacidad del individuo por ejemplo al evidenciar alguna enfermedad.
- Interoperabilidad: el hecho de usar diferentes sensores puede impedir el correcto funcionamiento de un sistema.

2.3.3. SISTEMAS BIOMÉTRICOS EN LA SOCIEDAD

La sociedad es la que determina el éxito de los sistemas en los mercados, como no podía ser de otra forma, este es el caso de los sistemas de identificación basados en rasgos biométricos.

La facilidad y comodidad en la interacción con el sistema contribuye a su aceptación. Si un sistema biométrico permite medir una característica sin necesidad de contacto directo, se percibe como más "amigable". Los rasgos biométricos que requieren colaboración del usuario suelen ser considerados incómodos y en cambio los sistemas que no requieren colaboración del usuario suelen ser considerados una amenaza a la privacidad de los usuarios.

Este último tema es de gran importancia en la biometría ya que al tratarse de estudio del individuo, puede revelar afecciones, enfermedades y podría ser utilizada esta información con fines poco éticos.

Pese a lo anterior los sistemas biométricos están considerados como uno de los medios más efectivos para la protección de la identidad, ya que la mayoría de los sistemas biométricos **no almacenan las características físicas** en su forma original, sino que almacenan una representación digital en un formato encriptado.

2.4. FUNCIONAMIENTO DE LOS SISTEMAS BIOMÉTRICOS

2.4.1. ESTRUCTURA GENERAL

Los sistemas de reconocimiento automático basados en rasgos biométricos poseen una estructura funcional común formada por varias fases cuyos procedimientos dependen de la naturaleza del rasgo a reconocer.

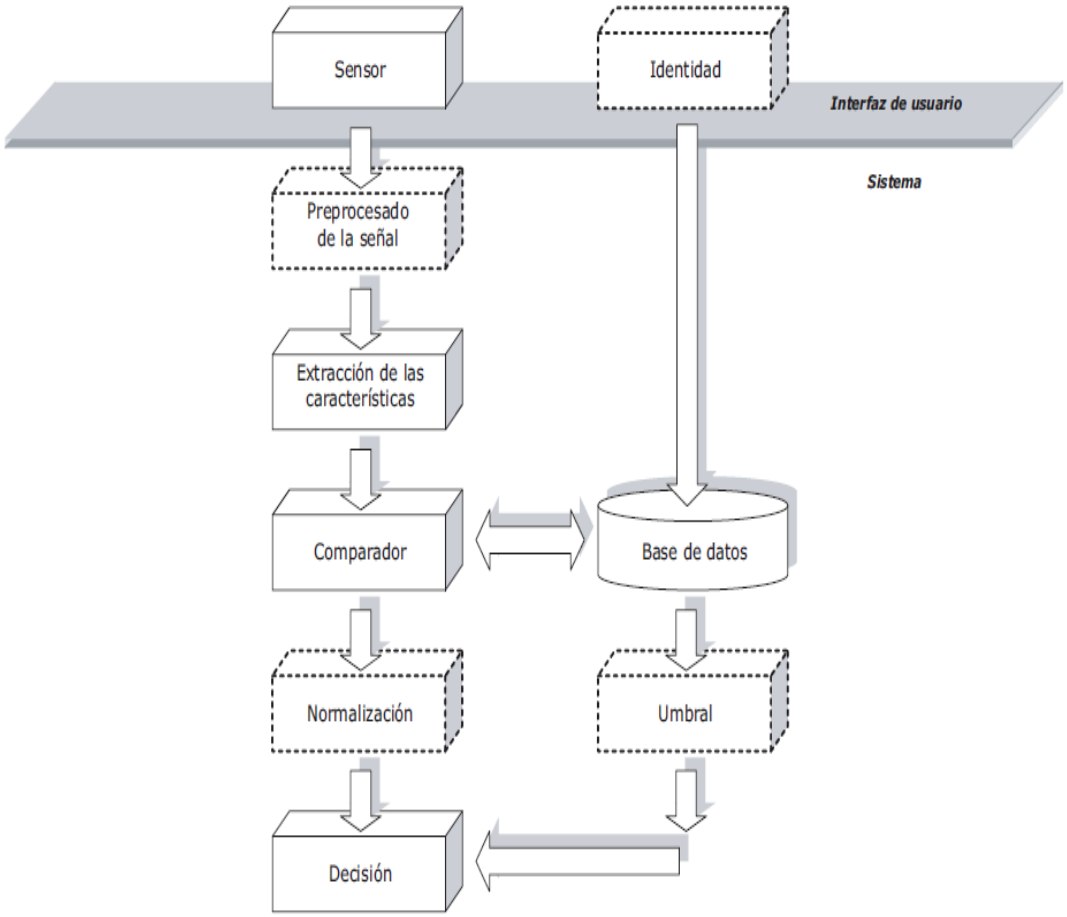


Figura 2. Cuadro general de funcionamiento de un sistema biométrico

Podemos resumir el esquema mostrado en la figura 2 agrupando las funcionalidades en 4 grandes grupos:

- **Adquisición de datos:** Se recogen los datos analógicos de partida (muestra biométrica) a través de un sensor y se convierten a formato digital.
- **Preprocesado:** En algunos rasgos es necesario acondicionar la información capturada para eliminar ruidos o normalizar la información para poder tener mejor rendimiento.

- **Extracción de características:** Se elimina la información no útil, aquella que no es específica del individuo o redundante. Se extraen las características discriminativas del individuo.
- **Comparación de patrones:** Una vez extraídas las características más discriminativas se comparan con el modelo o modelos de identidad almacenados en la base de datos del sistema utilizando umbrales de puntuación de similitud.

2.4.2. MODOS DE OPERACIÓN

Distinguiremos 2 modos de operación de los sistemas biométricos (**verificación e identificación**).

El modo **identificación** consiste en la búsqueda en la base de datos del sistema el modelo de usuario cuyas características sean muy parecidas al de la muestra de entrada.

El modo **verificación** consiste en la validación de la identidad de una persona comparando su rasgo biométrico capturado con su propia plantilla biométrica almacenada con anterioridad en la etapa de registro.

En el presente proyecto nos centraremos en el estudio de sistemas biométricos funcionando en modo verificación en el que la salida de la operación suele ser un valor de similitud entre las dos plantillas comparadas. Usando estos datos podemos observar dos tipos de errores:

FAR (False Aceptance Rate): Indica la probabilidad de que el sistema considere dos rasgos de individuos diferentes como provenientes del mismo usuario.

FRR (False Reject Rate): Indica la probabilidad que dos muestras provenientes del mismo individuo sean identificadas como de usuarios distintos por el sistema.

Al representar la FAR y la FRR frente a la puntuación de similitud (score) devuelto por el sistema se obtienen curvas como las mostradas en la figura 3. El punto de cruce entre la FRR y FAR se denomina **EER (Equal Error Rate)** punto en el que el error de falsa aceptación y falso rechazo se hacen iguales. Es un punto que suele utilizarse como medida del rendimiento del sistema

Dependiendo de la funcionalidad que se quiera para nuestro sistema biométrico convendrá buscar puntos umbral que nos permitan operar con un índice de falsa aceptación muy bajo (sistemas de alta seguridad) o FRR baja (alta conveniencia para el usuario).

En la figura 3 aparecen también ZeroFRR y el ZeroFAR, son respectivamente el punto de FAR donde obtenemos FRR cero y el punto del FRR donde la FAR se hace cero.

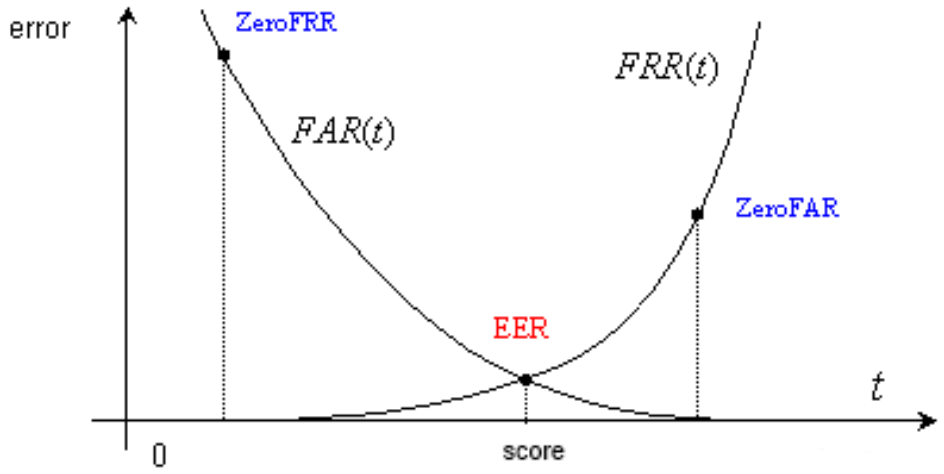


Figura 3. Ejemplo de curvas de FAR, FRR y obtención del EER.

3. SISTEMAS DE RECONOCIMIENTO DE IRIS

3.1. INTRODUCCIÓN

La utilización del ojo humano en la identificación de personas ha dado lugar a dos técnicas biométricas diferentes: una basada en el iris ocular y otra que utiliza las características distintivas de la retina. La única característica que tienen en común es que forman parte del mismo órgano y ambas se consideran como una técnica denominada biometría del ojo.

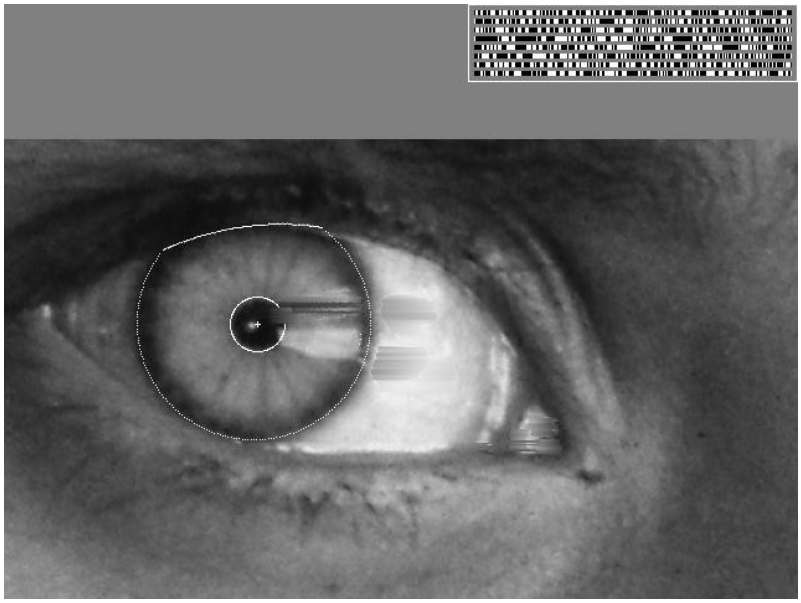


Figura 4. Ejemplo del análisis llevado a cabo por los sistemas de reconocimiento de iris, segmentación y codificación.

Como ya se adelantó antes (sección 2.2), la textura del iris es de gran utilidad debido a su carácter casi permanente e inalterable, presentando una alta variación entre clases y baja variación intraclase, lo cual le ha dado el estatus de uno de los métodos biométricos más fiables ya que se estima que la probabilidad de encontrar dos personas con el mismo patrón de iris es casi nula [30]. La potencialidad del iris para la identificación radica en una serie de características propias, como son la estabilidad frente a cambios, constituir un sencillo mecanismo de detección de sujeto vivo, la captura de datos (toma de imágenes) cada vez menos invasiva o la dificultad de falsificación.

3.2. EVOLUCIÓN EN EL TIEMPO

El concepto de identificación de humanos a través de su iris tiene más de 100 años de antigüedad [31]. Sin embargo la idea del reconocimiento de iris automático es algo más reciente, data de 1936 por el oftalmólogo Frank Burch.

Desde la década de los 80, ha aparecido en diversas películas de ficción (007, misión imposible, Los ángeles de Charlie, Minority Report…). Pero no es hasta 1985, cuando los oftalmólogos Leonard Flom y Aran Safir patentaron el concepto de Burch, exponiendo que no había dos iris semejantes [32].

Su incapacidad para poder desarrollar el sistema les condujo a contactar con el Dr. Jhon G. Daugman para desarrollar el algoritmo [33]. En 1993, la agencia comenzó a desarrollar el proyecto, en 1995 fue terminado con éxito y en 1994 se concedió la patente al Dr. Daugman y este sistema se convirtió en la base de la inmensa mayoría los sistemas comerciales de reconocimiento de iris existentes.

A partir de 2005, con la patente, que cubría el concepto básico de reconocimiento de iris, expirada se produjo un aumento en el mercado de sistemas de seguridad basados en iris ya que la finalización de la patente permitió a otras empresas no asociadas a los anteriores doctores introducirse en el mercado con sus propios algoritmos.

3.3. EL OJO Y SU ANATOMÍA

El ojo posee una lente llamada cristalino ajustable según la distancia, un diafragma (pupila) cuyo diámetro está regulado por el iris y un tejido sensible a la luz, la retina. La luz penetra a través de la pupila, atraviesa el cristalino y se proyecta sobre la retina, donde se transforma gracias a unas células llamadas fotorreceptoras en impulsos nerviosos que son trasladados a través del nervio óptico al cerebro.

Su forma es aproximadamente esférica, mide 2,5 cm de diámetro y está lleno de un gel transparente llamado humor vítreo que rellena el espacio comprendido entre la retina y el cristalino.

En la porción anterior del ojo se encuentran dos pequeños espacios: la cámara anterior que está situada entre la córnea y el iris, y la cámara posterior que se ubica entre el iris y el cristalino. Estas cámaras están llenas de un líquido que se llama humor acuoso, cuyo nivel de presión llamado presión intraocular es muy importante para el correcto funcionamiento del ojo.

Para que los rayos de luz que penetran en el ojo se puedan enfocar en la retina, se deben refractar. La cantidad de refracción requerida depende de la distancia del objeto al observador. Un objeto distante requerirá menos refracción que uno más cercano. La mayor parte de la refracción ocurre en la córnea, que tiene una curvatura fija. Otra parte de la

refracción requerida se da en el cristalino. El cristalino puede cambiar de forma, aumentando o disminuyendo así su capacidad de refracción.

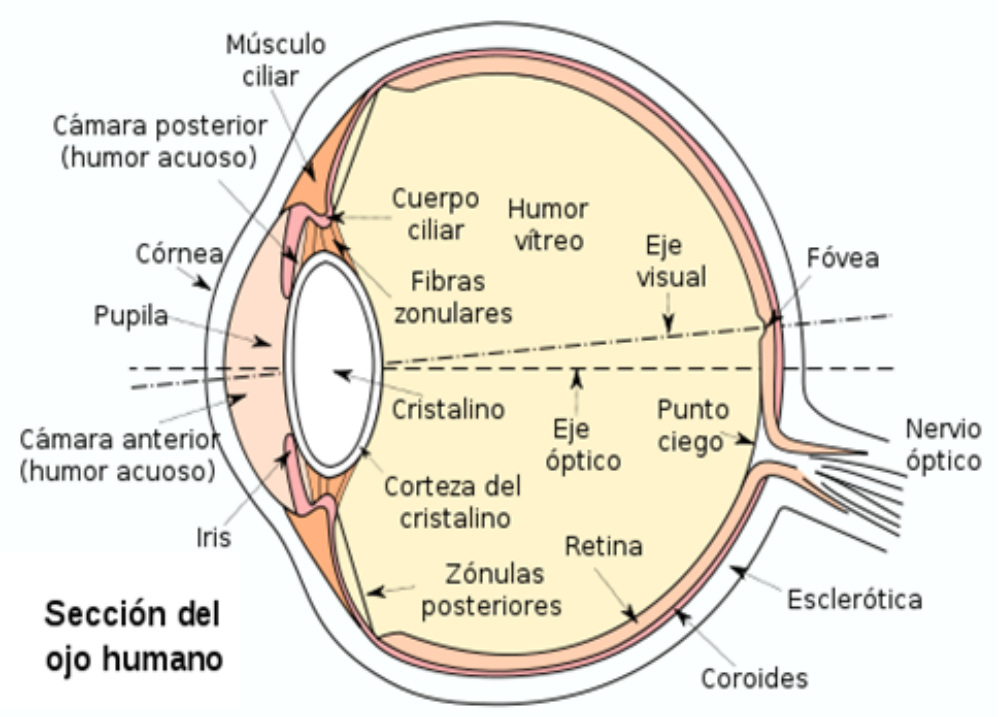


Figura 5. El ojo y su anatomía, partes del ojo.

3.3.1. ASPECTOS DIFERENCIADORES DEL IRIS

La estructura del iris de cada ojo muestra alto grado de unicidad y estabilidad con el tiempo. El patrón se mantiene prácticamente invariante desde la infancia del individuo. La herencia genética sólo determina la estructura general, pero no la estructura de detalle (pigmentación y tamaño de la pupila) que se estabiliza a partir de la adolescencia. Solo durante la vejez se observa una ligera despigmentación y una disminución de la apertura pupilar media. Sobre estos últimos datos, no existen pruebas exhaustivas sobre grandes poblaciones, por lo tanto no son concluyentes. En la Figura 7 podemos observar un ejemplo conocido de la poca variabilidad del iris humano con a la edad.

El iris contiene células pigmentadas y musculares y consta de cuatro capas que le permiten al iris ser distinto entre dos individuos:

- Membrana limitante anterior formada por fibroblastos y melanocitos estrellados.
- El estroma, capa de tejido fibroso constituido por colágeno en su mayor parte, contiene microblastos ahusados, capilares sanguíneos, nervios y macrófagos pigmentados. Alrededor de la pupila el estroma termina en el músculo esfínter de la pupila.
- Capa del músculo dilatador del iris se extiende desde la base del iris hasta el esfínter de la pupila.

- Epitelio posterior pigmentado, compuesto por dos capas de células pigmentadas con melanina.

El color del ojo se debe al número de células pigmentadas presentes en el estroma. Cuando hay pocas el color del ojo será azul, en los caso de albinismo, los microblastos pigmentados carecen de melanina y el iris aparece de color rojo debido a los capilares sanguíneos. En la Figura 6 se pueden observar diferentes pigmentaciones de iris.

Figura 6. Diferentes colores de iris dependiendo del número de células pigmentadas

Figura 7. Ejemplo de identificación de una persona gracias a sus ojos

En la figura 7 podemos observar un ejemplo muy conocido, una persona localizada 18 años después gracias al análisis de sus ojos. La revista National Geographic buscó a una joven que había fotografiado 18 años atrás y gracias a los análisis de el Dr. J. Daugman consiguieron localizar a la protagonista de la portada 18 años atrás. Los análisis demostraron que la posibilidad de error para el ojo izquierdo era de 1 de 6 millones y para el derecho una de 10^{15}.

3.4. ADQUISICIÓN DE IMÁGENES DE IRIS

El primer esquema propuesto para la adquisición del iris se trataba de un sistema que controlaba la iluminación mediante cuatro puntos de enfoque, la reflexión producida por el ojo en una lente proporcionaba la imagen buscada. En la Figura 88 mostramos el sistema propuesto por los doctores Flom y Safir en 1987 basado en la iluminación directa y captura de la imagen frontalmente.

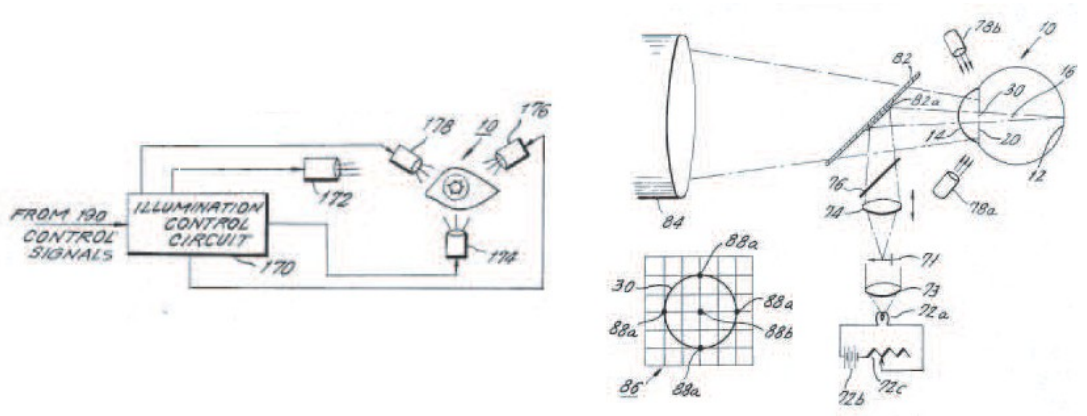
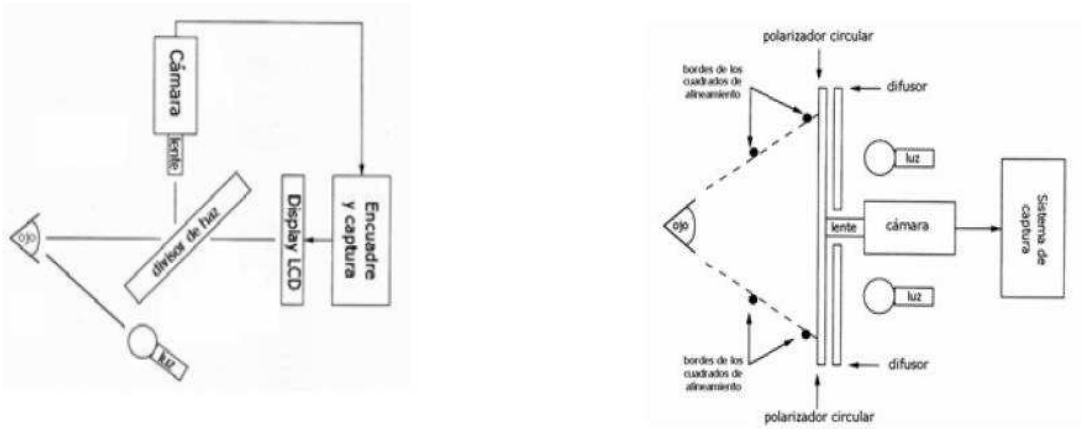


Figura 8. Esquema propuesto por Flom y Safir en 1987

Posteriormente surgieron los sistemas de Daugman y Wildes que funcionaban capturando la imagen con el reflejo en un espejo, después de haber iluminado el ojo de forma diagonal (Daugman) o iluminando con dos puntos de luz y colocando la cámara enfrente al ojo. En la Figura 9 podemos observar los sistemas propuestos por Daugman y Wildes.



(Sistema Daugman) *(Sistema Wildes et al)*

Figura 9. Sistemas de captura del iris de Daugman (izquierda) y Wildes (derecha).

En ambos sistemas los niveles de iluminación son bastantes bajos. Para confort del usuario, se suelen realizar aperturas de diafragma relativamente grandes con poca profundidad de campo. Ambos sistemas aprovechan las ventajas que proporciona la toma de secuencias de imágenes capturándose una secuencia de vídeo y eligiendo la mejor imagen.

Aun con estos sistemas, es necesario que el usuario sea cooperativo ya que si no el posicionamiento del iris se puede ver afectado por problemas de oclusión, desviación de ángulo, etc.

3.4.1. SISTEMAS COMERCIALES DE ADQUISICIÓN

La implantación de sistemas de reconocimiento es cada vez mayor en nuestra sociedad. Poco a poco el mundo de la biometría comienza a introducirse en nuestra vida cotidiana, permitiéndonos acceso a múltiples aplicaciones gracias a nuestros rasgos biométricos. En este sentido los sistemas biométricos de iris están cobrando gran relevancia, por tratarse de sistemas de alta seguridad.

Un ejemplo de implantación privado es el uso en aeropuertos para la identificación de viajeros, este es el caso del aeropuerto de Heathrow, que permite la identificación de viajeros en tiempo real sin necesidad de comprobar adicionalmente el pasaporte.

Otro ejemplo de implantación es en ámbito militar, implantado en el control de fronteras o en identificación de terroristas.

Actualmente se ha desarrollado un software que permite actuar como sensor de iris cualquier aparato con un mínimo procesador que posea una cámara con una resolución de por lo menos 2Mpixes.

3.4.2. FACTORES DE CALIDAD

Debido a la naturaleza del proceso de adquisición se pueden dar por diversos motivos imperfecciones en la imagen capturada. Por ello en la literatura se proponen medidas de calidad para discernir si una imagen es válida para su análisis o si es necesario adquirir una nueva.

Existen muchas medidas de calidad propuestas en la actualidad. Se pueden hacer diferentes agrupaciones en clases ateniendo a lo que miden, o los operadores que utilizan, para este trabajo hemos decidido agruparlas según la característica que quieren medir, en base a ellas en la figura 10 observaremos una imagen que cumple los mínimos de calidad vs otra que no lo hace:

- **Medidas de oclusión:** miden la zona del iris disponible a ser analizada que no es tapada por párpados, pestañas u otros elementos.
- **Medidas de borrosidad:** miden la borrosidad de la imagen debido al movimiento del ojo en el momento de la captura o al enfoque de la cámara que realiza la captura.
- **Medidas de contraste:** miden los cambios en la escala de grises de las imágenes a imagen a ser analizadas.
- **Medidas de dilatación:** miden la relación entre iris y pupila.

- **Medidas de desalineamiento angular:** mide la inclinación del ojo hacia algún lateral de la imagen en la captura.

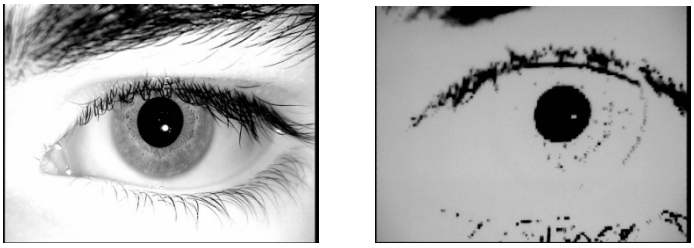


Figura 10. Imagen de calidad vs imagen que no cumple los mínimos de calidad.

Estas medidas surgen como una ayuda al procesado de la imagen ya que para poder segmentar una imagen de iris o poder hacer otras operaciones necesarias para la identificación o verificación de una imagen, son necesarios unos mínimos de calidad, sino sería imposible el análisis.

3.4.3. LOCALIZACIÓN, SEGMENTACIÓN DEL IRIS Y MATCHING

El procedimiento automático de localización se basa en detectar los círculos interior y exterior del iris que definen sus bordes. El proceso en si es una tarea compleja, puesto que la forma del objeto a segmentar no tiene una forma regular y sus límites no están siempre bien definidos.

Existen diversos métodos y técnicas de segmentación. Inicialmente se centraban en modelar ambos, pupila e iris, como dos circunferencias concéntricas, pero las recientes investigaciones apuestan por el modelado irregular de dichos contornos.

La etapa de segmentación es fundamental para el éxito de un sistema de reconocimiento del iris, ya que los datos mal segmentados generan un patrón de iris corrupto, lo que provocará errores de reconocimiento. El éxito de la segmentación depende de la calidad de la imagen en base a tres puntos clave:

- Sensibilidad a una alta gama de contrastes entre los bordes.
- Robustez ante irregularidades en los bordes.
- Capacidad de considerar aperturas y cierres pupilares variables

Gracias a estos puntos podremos realizar una segmentación óptima, como la mostrada en la figura 11.

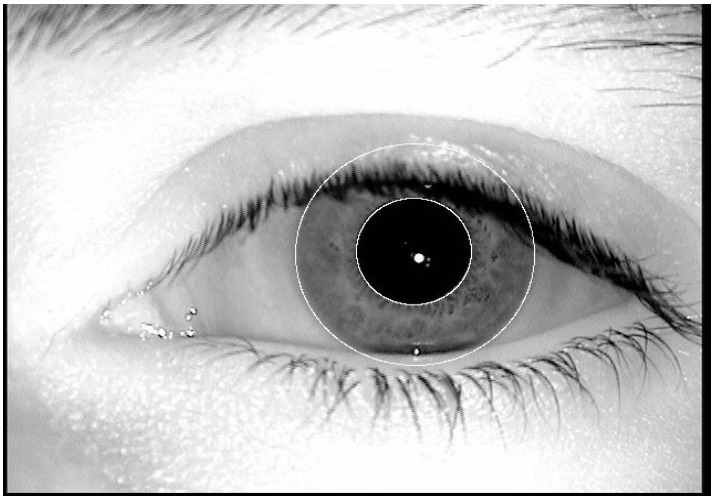


Figura 11. Ejemplo de detección de la corona circular del iris.

Uno de los métodos más utilizados es el método Daugman, la primera metodología efectiva implementada en el reconocimiento biométrico del iris. Comprende una serie de operaciones integro-diferenciales para la localización de los bodes circulares de la pupila y el iris.

Otra metodología utilizada es la de Wildes, realiza la búsqueda de contornos en dos pasos:

- Obtención de una imagen de bordes binaria (solo blanco y negro) mediante el cálculo del módulo del vector gradiente.
- Detección de los contornos circulares mediante rotación por transformada de Hough.

Además de estos métodos existen en la actualidad otros también muy válidos, Bonney [34] prelocaliza la pupila usando operaciones de dilatación y compresión de la imagen y una vez encontrada calcula la desviación estándar en vertical y horizontal para lograr obtener los límites de pupila e iris. El-Bakry [35] propuso la utilización de redes neuronales para la segmentación del iris, Tuceryan [36] propone un método basado en un algoritmo de segmentación de texturas.

Una vez segmentado el iris se procede a normalizar el tamaño, consiste en convertir la corona circular seleccionada en un rectángulo, este será el que posteriormente se codifique y permita la comparación entre plantillas (matching). En la figura 12 podemos observar el resultado del procesado del iris según el proceso de Daugman.

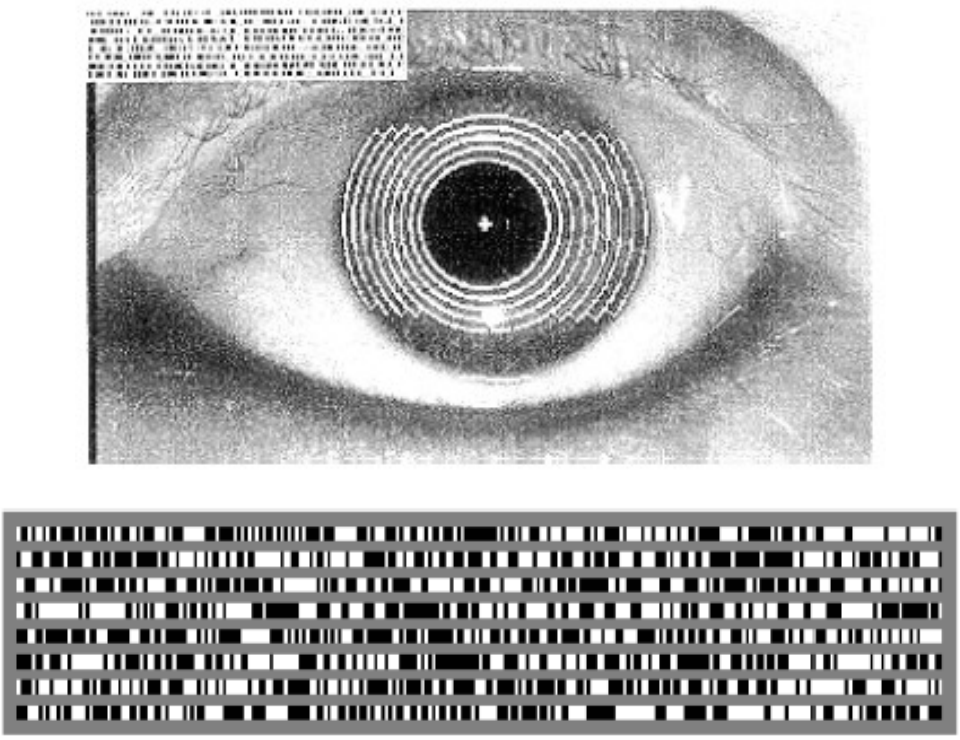


Figura 12. Extracción de la información de la corona circular del iris en el código patrón rectangular.

Una de las codificaciones más utilizadas, propuesta por Daugman es la aplicación de los filtros de Gabor, que se construyen a través de la modulación de una onda senoidal/cosenoidal como una gaussiana. Además de la propuesta de Daugman, existen otras codificaciones como son la Log-Gabor, Wavelets, Haar Wavelet o la DCT.

La comparación de patrones (pattern matching) implica el proceso de reconocimiento de iris sigue cuatro pasos diferentes:

- Alineamiento espacial de patrones a comparar.
- Representación paramétrica de la información diferenciada de los patrones.
- Evaluación de la bondad de comparación (similitud)
- Decisión de reconocimiento (aceptación o rechazo en función de un valor umbral)

Para la evaluación de similitud en este proyecto se ha realizado mediante la distancia Hamming entre los dos patrones, que es el método más extendido en la literatura.

4. ATAQUES A SISTEMAS AUTOMÁTICOS DE RECONOCIMIENTO DE IRIS

Dentro del campo de los sistemas de seguridad basados en iris, debido a tratarse de un sistema de alta seguridad, tiene gran relevancia el estudio de sus vulnerabilidades a ataques externos.

Como todo sistema de seguridad siempre ha habido intentos de engañar al sistema para acceder a la información que protege. El desarrollo de las técnicas de seguridad va unido al desarrollo de los ataques a los sistemas, esto es, cuanto mejor es el sistema de seguridad, más sofisticado debe ser el método de ataque al sistema para lograr burlarlo y viceversa, cuanto más sofisticados sean los métodos de ataque a los sistemas, más robustos necesitaremos que sean.

Dentro de los ataques a sistemas biométricos encontramos dos grandes grupos:

Ataques directos: aquellos que se llevan a cabo directamente sobre el sensor, como puede ser con guantes de plástico para huella dactilar o las lentes de contacto para el iris.

Ataques indirectos: aquellos que se llevan a cabo en alguna de las partes internas del sistema ya sea en el procesado o en el matching (identificación del parecido de la muestra a la de referencia).

4.1. ATAQUES DIRECTOS A IRIS

Los principales ataques directos a sistemas basados en iris son mediante réplicas de los iris de los usuarios originales del sistema, hasta la actualidad se conocen diversos métodos que van desde la fotografía de alta calidad del ojo del usuario, un vídeo, uso de lentes de contacto o incluso generación de imágenes sintéticas de iris a través de ordenador.

Thalheim [45] , presentó una forma de atacar al sistema automático de reconocimiento de iris con imágenes impresas en alta resolución, para poder pasar la seguridad del sistema recortaba la pupila y la sustituía por la del ojo del impostor poniéndose este detrás del papel para dar la impresión al sistema de que era un ojo real.

Matsumoto [1] realizó unos experimentos similares, esta vez se testearon 3 sistemas de verificación. Dos aparatos diferentes fueron utilizados para adquirir las imágenes de los falsos iris. Las imágenes capturadas fueron impresas utilizando una impresora de alta resolución y se sustituyó (al igual que Thalheim) la pupila impresa por la del impostor. Los tres sistemas fueron engañados y los investigadores pudieron acceder con las imágenes falsas.

Estos dos investigadores mostraron la posibilidad de engañar al sensor con este método simple el cual solo requiere una impresión de calidad de la imagen del iris.

V.Ruiz-Albacete [12] desarrolló una base de datos de falsos iris utilizando impresiones de alta calidad de imágenes de iris sobre tres tipos diferentes de superficies de impresión. Consiguió un alto porcentaje de engaño al sensor y sin necesidad de sustituir la pupila de la imagen por una real.

Seelen propone [28] el uso de lentes de contacto, aunque también muestra en su estudio la forma de detectarlos mediante el análisis de la transformada de Fourier en 2D.

Además de estos intentos, los investigadores han realizado ataques a los sistemas de iris mediante impresiones de calidad [46], lentes de contacto [5] o incluso sofisticadas construcciones 3D de iris artificiales [24].

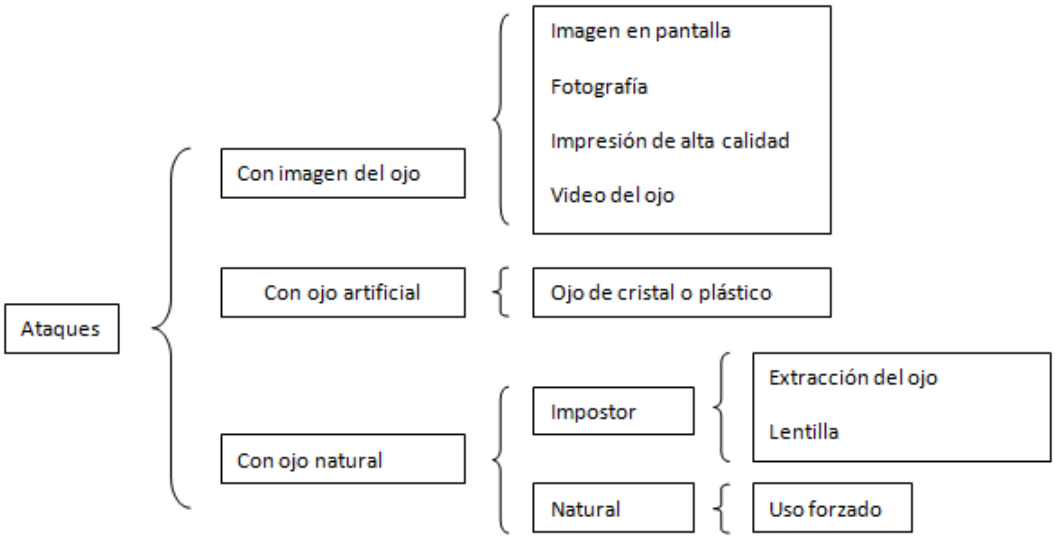


Figura 13. Clasificación de ataques directos según Bori Toth y Ulf Cahn con Seelen [37]

En la figura 13 observamos los diferentes ataques directos, aparecen algunos ya comentados como los ataques de Matsumoto, Talheim y V.Ruiz-Albacete con impresiones de alta calidad, el uso de lentes de contacto de Seelen o el uso de ojos artificiales y aparecen nuevos, no nombrados antes, como son el uso de vídeos o el uso de propio órgano ya sea por amputación o uso forzado.

4.2. ATAQUES INDIRECTOS A IRIS

En los ataques indirectos, al igual que en el resto de sistemas de seguridad basados en biometría, se necesita acceso al sistema y cierto conocimiento de sis módulos internos (formato de las plantillas, matcher…). Para este objetivo se suele trabajar con troyanos y virus que una vez en el sistema pueden enviarnos información interna y burlarlo sin ser

detectados, pudiendo cambiar los valores de las medidas llevadas a cabo, de los algoritmos de matching o incluso la decisión final el clasificador.

Aunque sí que existen diversos trabajos de ataques indirectos a otros rasgos como huella dactilar [47, 48] o cara [49], en iris sólo se ha publicado hasta la fecha un trabajo en el que se lleva a cabo este tipo de ataques [50].

4.3. PROTECCIÓN FRENTE A ATAQUES DIRECTOS: LIVENESS DETECTION

Ante la existencia de ataques directos a los sistemas de seguridad, los investigadores proponen y llevan a cabo una serie de contramedidas.

Una de las propuestas es el uso de varias características biométricas (multimodalidad), así un sistema que base su trabajo (identificación o verificación) en reconocimiento facial e iris será más robusto y más difícil de engañar que un sistema que solo utilice para su modo de operación de los rasgos [38].

Otra de las principales vías para la lucha contra los ataques directos en iris es la detección de vida (*"liveness detection")*.

El principal objetivo en *"liveness detection"* es conseguir clasificar una muestra de un ojo como real (original) o falso (sintético).

Para esta memoria, las diversas técnicas de *"liveness detection"* han sido agrupadas en **métodos hardware** (aquellos que necesitan de elementos adicionales para hacer la detección de vida) y **métodos software** (aquellos que no necesitan más que la imagen capturada por el sensor para establecer la característica de vida del ojo situado). No obstante existen otras formas de clasificarlas como son entre métodos pasivos y métodos activos dependiendo de la interacción o no, del usuario (como puede ser pedir al usuario que mueva el ojo, que mueva los parpados, modificar la iluminación drásticamente…) [41].

A continuación procedemos a mostrar la clasificación de los métodos de "*liveness detection*" en métodos hardware y software:

4.3.1. MÉTODOS HARDWARE

Los métodos hardware son aquellos que se valen de elementos adicionales al sensor para la detección de la originalidad del ojo frente al sensor. Para ello miden comportamientos involuntarios del órgano como son la detección del *hippus* de la pupila (oscilación permanente de la pupila bajo condiciones de iluminación uniforme), la respuesta una iluminación repentina (con un diodo por ejemplo)[16], medir los reflejos infrarrojos de la córnea[3] o reflexión en la retina entre otras medidas propuestas. Además podemos medir comportamientos voluntarios del ojo, como previamente se ha comentado en la introducción como son el parpadeo o el movimiento del ojo bajo demanda.

J. Daugman propuso [42] la detección de vida mediante la observación de una serie de comportamientos del ojo:

- Comportamientos voluntarios: comportamientos del ojo realizados de forma voluntaria pro el usuario, el usuario mueve el ojo o parpadea bajo demanda del sistema.
- Comportamientos involuntarios: aquellos que el ojo realiza sin que el usuario haga nada voluntariamente, como son el *hippus* de la pupila ante una iluminación constante o la respuesta de la pupila ante cambios de iluminación [40].

4.3.2. MÉTODOS SOFTWARE

En este caso los falsos iris son detectados una vez que la muestra ha sido adquirida con el sensor y son preferidos debido a su menor coste y su menor grado invasivo con el usuario. Los principales métodos son la detección de las cuatro reflexiones de Purkinje [23], la detección de lentes de contacto impresas a partir del análisis de las textura de grises [5], el análisis del brillo de la imagen [22], el análisis de la transformada 2D de Fourier u otras transformadas:

J. Daugman [16] propuso una serie de medidas espectrográficas de propiedades de partes del ojo (tejido, grosor, pigmentación..), la reflexión de la alineación coaxial (efecto ojos rojos) y las cuatro reflexiones de Purkinje [23].

Schukers propuso varias formas de hacer la detección de vida basándose en (1) la información de vida inherente a la característica biométrica, (2) mediante información adicional proveniente del procesado de la captura del sensor.

Los investigadores X.He, S. An y P. Shi propusieron la medida de características basadas en la matriz de coocurrencia en escala de grises analizando la textura de la captura del sensor [39].

Por otro lado los investigadores Wei y Qiu [43] proponen el análisis de las textura de las imágenes para detectar el uso de lentillas, así calculan la nitidez de las imágenes y otros factores que les ayudan a detectar los falsos ojos (en este caso usando lentillas).

Otra forma propuesta en la literatura de identificación de ojos falsos es mediante un paquete de wavelets de transformada (similar a la transformada de Fourier) y análisis del espectro transformado [44].

Además de todos estos métodos reconocidos ha surgido, en otros rasgos biométricos, la idea de relacionar la calidad de las imágenes capturadas por el sensor (en cuanto a criterios de calidad establecidos previamente) con su naturaleza sintética u original. En el caso de huella dactilar, J. Galbally propone el sistema con un rendimiento en identificación de vida en huella dactilar bastante alto [8].

En este proyecto proponemos un sistema de detección de vida software basado en algoritmos de extracción de características de para identificar la originalidad de la imagen (real o falsa) de entrada.

5. SISTEMA DE DETECCIÓN DE VIDA DESARROLLADO

El problema de la detección de vida que se ha afrontado en este proyecto se puede ver como un problema de clasificación de dos clases donde la entrada es una imagen de iris y tiene que ser asignada a una de las dos clases: real o sintética (falsa).

La clave de la cuestión es encontrar un conjunto discriminativo de características en el proceso que permita construir un clasificador apropiado que se capaz de identificar la imagen como real ó sintética.

En este trabajo se ha extraído como conjunto de rasgos distintivos una serie de medidas de calidad como las introducidas en el apartado 3.4.2.

Así pues, en este trabajo se propone una novedosa parametrización utilizando medidas de calidad, aplicada y testeada en un sistema completo de detección de vida.

5.1. ESTRUCTURA DEL SISTEMA

Como se puede observar en la figura 14, la entrada al sistema es una imagen de iris (la misma muestra que usaría el sistema de identificación biométrico).

En el primer paso se segmenta la imagen del ojo extrayendo centros de pupila e iris y radios mediante una transformada de Hough [12].

Una vez extraída esta información procedemos a extraer las 22 medidas de calidad implementadas en este proyecto, las más discriminativas. Posteriormente se seleccionan las mas discriminativas utilizando el algoritmo SFFS (Sequential Floating Feature Selection) propuesto por Pudil [27].

Una vez que el vector final de características ha sido generado se clasifica la muestra como real (proviene de un ojo original) o falsa (proveniente de un ojo sintético, es un intento de suplantación).

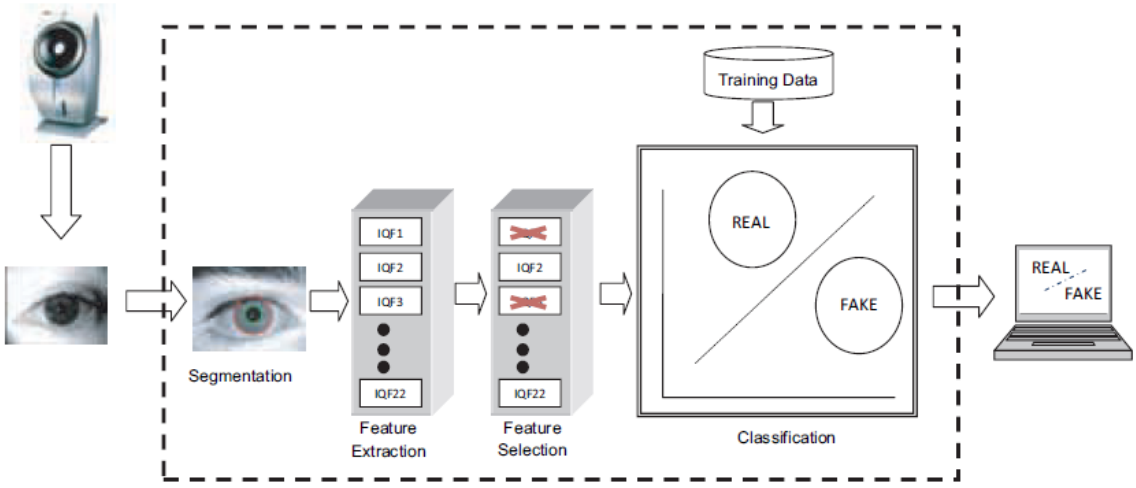


Figura 14. Diagrama general del sistema de detección de vida presentado en este proyecto.

En las siguientes secciones se detalla cada uno de los pasos que intervienen en el sistema:

5.2 PRARÁMETROS DE CALIDAD IMPLEMENTADOS

La parametrización propuesta en este trabajo y su aplicación a la detección de vida comprende 22 adaptaciones de características de calidad de diferentes parámetros descritos en la literatura (en la figura 14 aparecen como IQF: Iris Quality Features, es decir Medidas de Calidad del Iris).

Desde un punto de vista biométrico la calidad de las imágenes de iris pueden ser establecidas midiendo una de las siguientes propiedades:

- Enfoque.
- Emborronamiento por movimiento.
- Oclusión.
- Otros: incluyendo contraste o dilatación de la pupila.

Como se puede observar en la tabla 1, para cada característica se han implementado diferentes propuestas de la literatura calculando la potencia de las altas frecuencias de la imagen, dirección de ángulos utilizando filtros direccionales, intensidad de los pixeles en determinadas regiones, o diferentes relaciones entre los tamaños de la pupila y el iris.

La calidad de la imagen puede ser hallada analizando la imagen completa o combinando medidas de diferentes partes de la imagen. A cada una de las medidas las denominaremos MCI (Medida de Calidad del Iris)

Clase	Características
Enfoque	MCI1, MCI4, MCI15, MCI16
Movimiento	MCI2, MCI5, MCI18, MCI20
Oclusión	MCI3, MCI6-12, MCI17, MCI19, MCI21
Otros	MCI13, MCI14, MCI22

Tabla 1. Resumen de los 22 parámetros implementados en el trabajo, clasificados de acuerdo a la característica principal medida en la imagen.

A continuación se dan detalles sobre las medidas de calidad, implementadas en el trabajo, clasificadas según la tabla 1:

5.2.1 PARÁMETROS DE ENFOQUE

Intuitivamente una imagen con un buen enfoque es una imagen bastante definida y muy marcada. Por esto el desenfoque principalmente atenúa las altas frecuencias espaciales de la imagen, por ello los investigadores proponen medir el enfoque utilizando el análisis de las altas frecuencias, ya sea en alguna parte en especial de la imagen o en su totalidad.

Al final de este apartado, en la Figura 15, al final de la subsección, mostramos las diferencias entre ojos reales y sintéticos para estos parámetros:

- **Potencia de altas frecuencias 1 (MCI4)** [15], mide la concentración de energía de las componentes de altas frecuencias utilizando un filtro paso alto de convolución de 8x8:

-1	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**
-1	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**
-1	**-1**	**3**	**3**	**3**	**3**	**-1**	**-1**
-1	**-1**	**3**	**3**	**3**	**3**	**-1**	**-1**
-1	**-1**	**3**	**3**	**3**	**3**	**-1**	**-1**
-1	**-1**	**3**	**3**	**3**	**3**	**-1**	**-1**
-1	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**
-1	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**

  Posteriormente el valor de la medida a cada imagen se obtiene haciendo el sumatorio en dos dimensiones de la matriz resultante de la convolución y se divide el valor obtenido entre las dimensiones de la imagen.

- **Potencia de altas frecuencias 2 (MCI1)** [6]**,** muy similar al anterior el MCI4 pero utiliza una versión modificad del filtro paso alto, esta vez es de 5x5 [15].

$$\boldsymbol{MCI1} = \frac{\mathbf{1}}{\boldsymbol{M} \times \boldsymbol{N}} \sum\sum \boldsymbol{HFP}$$

Donde M y N son las dimensiones de la matriz HFP y la matriz HFP es el resultado de convolucionar la imagen con el núcleo de 5x5:

-1	**-1**	**-1**	**-1**	**-1**
-1	**2**	**2**	**2**	**-1**
-1	**2**	**0**	**2**	**-1**
-1	**2**	**2**	**2**	**-1**
-1	**-1**	**-1**	**-1**	**-1**

- **Potencia de altas frecuencias 3 (MCI16)** [6]**,** idéntico al anterior pero utilizamos otro núcleo de convolución para el filtrado paso alto, esta vez también es de 5x5:

-1	**-1**	**-1**	**-1**	**-1**
-1	**-1**	**4**	**-1**	**-1**
-1	**4**	**4**	**4**	**-1**
-1	**-1**	**4**	**-1**	**-1**
-1	**-1**	**-1**	**-1**	**-1**

- **Potencia de altas frecuencias 4 (MCI15)** [10]**,** estima el desenfoque de la imagen implementando la segunda derivada (usando una aproximación discreta del operador laplaciano) con la intención de filtrar en paso alto las imágenes de iris.

$$MCI15 = \frac{1}{X \times Y} \sum\sum F(x,y)$$

$$F(x,y) = \sum_{i=x-N}^{x+N} \sum_{j=y-N}^{y+N} \nabla^2_{ML}\,(x,y)$$

$$\nabla^2_{ML}(x,y) = |2I(x,y) - I(x-s,y) - I(x+s,y)| + |2I(x,y) - I(x,y-s) - I(x,y+s)|$$

En las fórmulas anteriores *X* e *Y* son las dimensiones de la imagen, N es el tamaño de la ventana de estudio para cada pixel, ∇^2_{ML} es el operador de variación lateral, *"s"* es el desplazamiento par el operador y *"x"* e *"y"* son las coordenadas de estudio en la imagen.

Para nuestras muestras de entrenamiento se ha observado que los valores óptimos para separar al máximo las distribuciones en este factor de calidad son S=21, N=1.

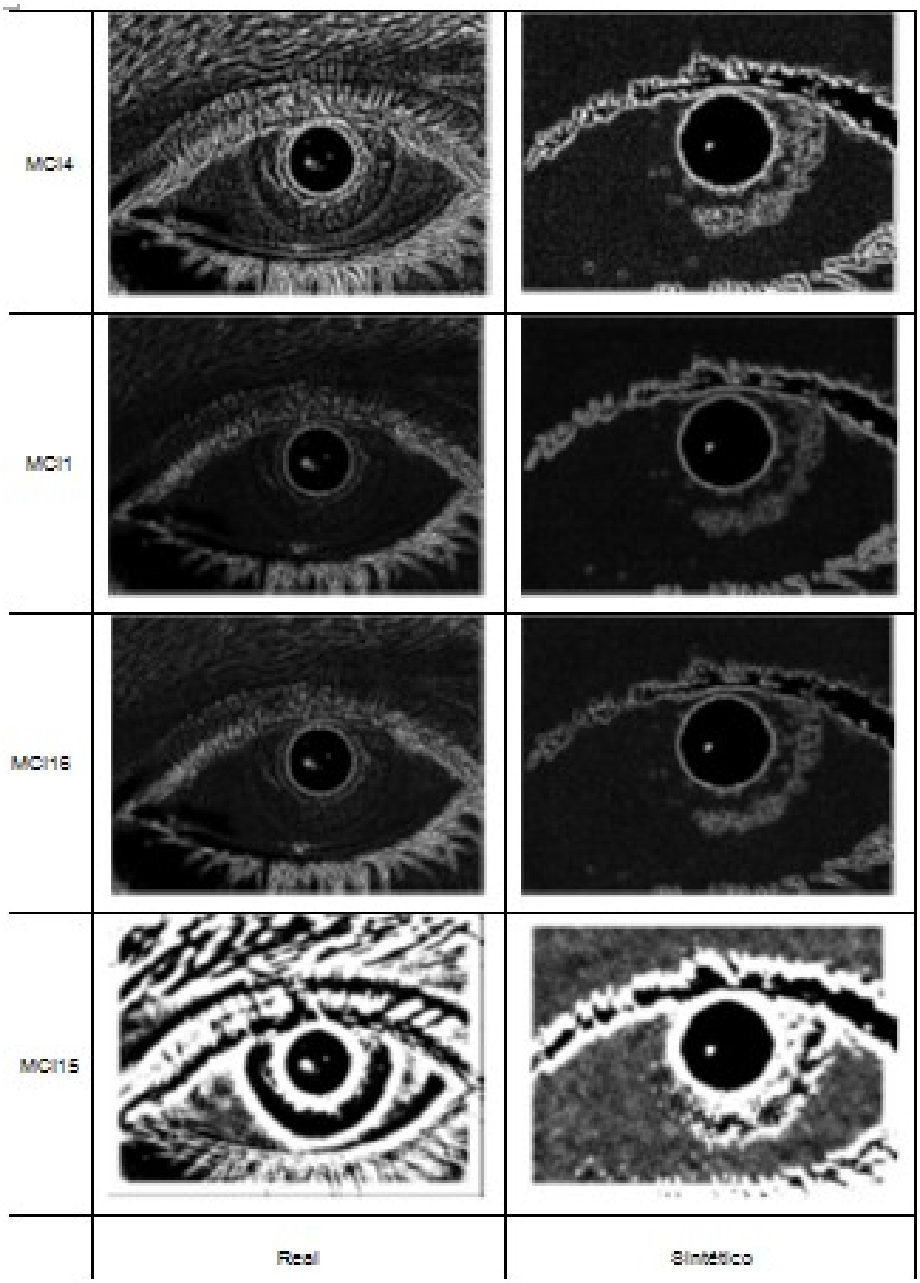


Figura 15. Ejemplo de computación de las diferentes medidas de enfoque implementadas para dos ojos, uno real y otro sintético.

La figura 15 muestra como sensiblemente existen diferencias apreciables a la vista entre las imágenes reales y sintéticas para las características de calidad MCI4 e MCI15. En cambio para las medidas MCI1 e MCI16 no se aprecian casi diferencias en el comportamiento entre la imagen original y la sintética.

5.2.2 PARÁMETROS DE MOVIMIENTO

Este tipo de características tratan de estimar la borrosidad causada por el movimiento (del ojo o del sensor). El efecto de movimiento es generalmente reflejado en la direccionalidad de la imagen, por ello las medidas suelen estar basadas en el cálculo de las direcciones dominantes en cada muestra de iris:

- **Potencia vertical de altas frecuencias 1 (MCI2)** [6]**:** usa el filtro SMD (Sum Modulus Difference) propuesto por Jarvis [20] para medir las altas frecuencias espaciales en la vertical como un indicador de borrosidad por movimiento.

  Para ello utiliza un núcleo de convolución con la imagen y posteriormente calcula el valor medio:

-1	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**	**-1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**

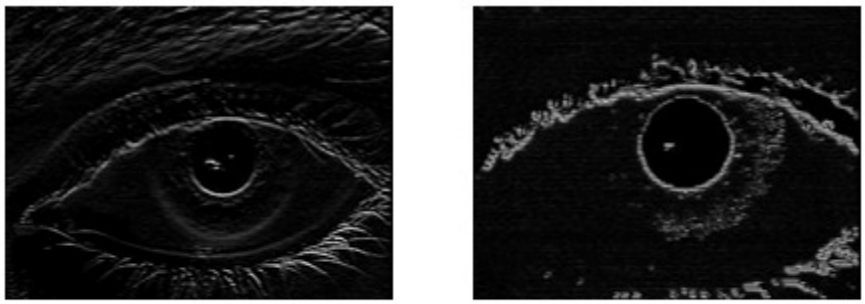


Figura 16. Potencia vertical de altas frecuencias 1. MCI2

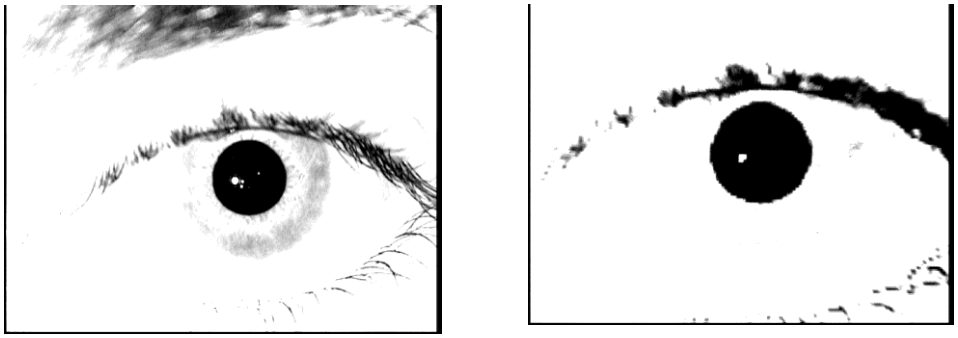
A simple vista, apreciamos en la imagen real mayor variación de grises, esto podría suponer una diferenciación entre los conjuntos real y sintético de imágenes. Pero para poder hacer esta afirmación de rigurosa, necesitamos hacer uso de los histogramas de valores de los conjuntos de imágenes y resultados (en la sección 0).

- **Potencia vertical de altas frecuencias 2 (MCI18)** [14]**:** Similar al anterior pero utiliza una nueva versión del filtro SMD. Para esta medida se aplica el siguiente proceso:

$$MCI18 = \frac{1}{M \times N} * \sum\sum F(x,y)$$

$$F(x,y) = I(x,y) - I(x,y-1)$$

Donde *I* es la imagen a tratar y *M* y *N* son sus dimensiones y *x* e *y* la posición medida en píxeles. En la figura 17 observamos las diferencias entre una imagen falsa y una original. Como se observa el SMD hace desaparecer en la imagen falsa la banda del iris



Real Sintético

Figura 17. Imágenes tratadas según la medida MCI18.

- **Fuerza direccional (MCI5) [21]:** Busca la dirección primaria de movimiento de la imagen usando mascaras direccionales (separadas 5 grados entre ellas) y obtiene la potencia espectral total de las imágenes filtradas resultantes.

  El siguiente paso, como es mostrado en la figura 18, es seleccionar aquella dirección que posea el mayor valor de potencia espectral (esta será la dirección dominante).

  Posteriormente el valor final de la medida es obtenido como la suma de los cuadrados de los coeficientes de Fourier del vector, de la transformada de la imagen, perpendicular de la dirección dominante.

Figura 18. Espectro de potencia de imágenes en sus direcciones primarias.

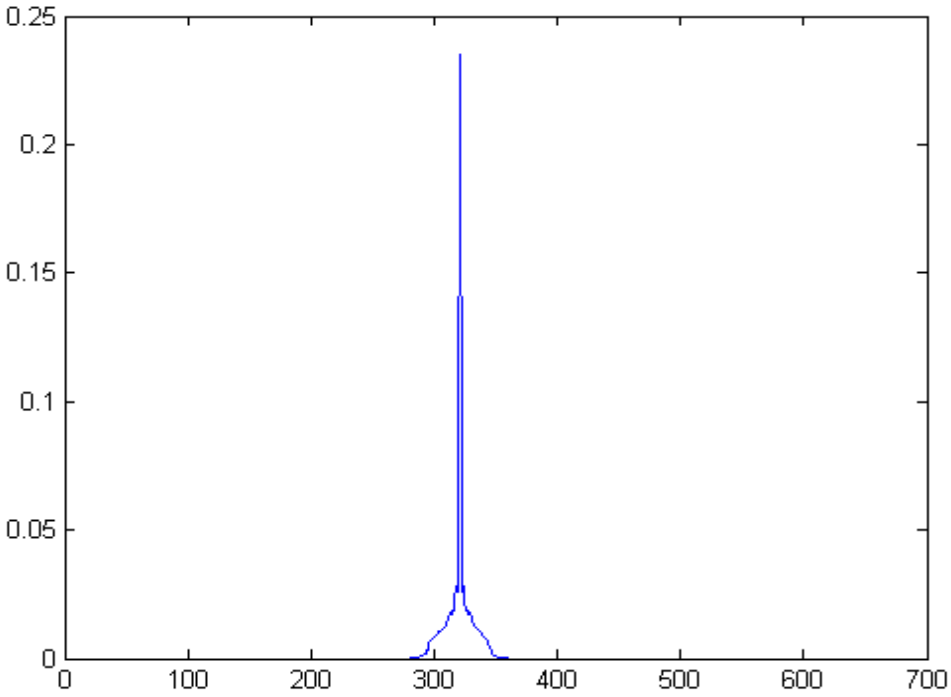


Figura 19. Serie de valores de los coeficientes de Fourier.

En la figura 19 observamos la serie de valores de los coeficientes de Fourier correspondiente a la perpendicular de la dirección predominante en la imagen, calculada usando las máscaras direccionales.

Para este algoritmo surgió la duda de comparar una imagen original con su falsificación en iguales condiciones, es decir, para cada imagen y su falsificación analizar la misma dirección. No obstante el análisis que se realiza en este proyecto es estadístico y no por parejas, por ello no creímos que fuese necesario implementar

para esta medida el análisis de la las imágenes por parejas, sino que el análisis individual es el apropiado.

Esta última afirmación lo hacemos en consonancia con el objetivo del proyecto, que es **un algoritmo que sea capaz de, con una sola muestra, identificar la imagen como real o sintética**. Por esto no podemos plantearnos analizar las imágenes falsas en relación con sus supuestas originales, ya que el atacante al sistemas no nos va a proporcionar previamente la muestra original que planea suplantar.

- **Información de espectro global (MCI20)** [29]**:** estima el movimiento y la borrosidad simultáneamente considerando información espectral total de la imagen y la relación entre aérea de iris y total de la imagen (hace uso para ello del MCI19).

5.2.3 PARÁMETROS DE OCLUSIÓN

Estas medidas tratan de de detectar qué áreas del iris están ocluidas por algún elemento externo como son los párpados o las pestañas.

Región de interés (MCI3) [6]**:** Analiza el valor medio de los píxeles en una región situada 50 píxeles sobre el centro de la pupila. Este procedimiento se muestra en la siguiente figura.

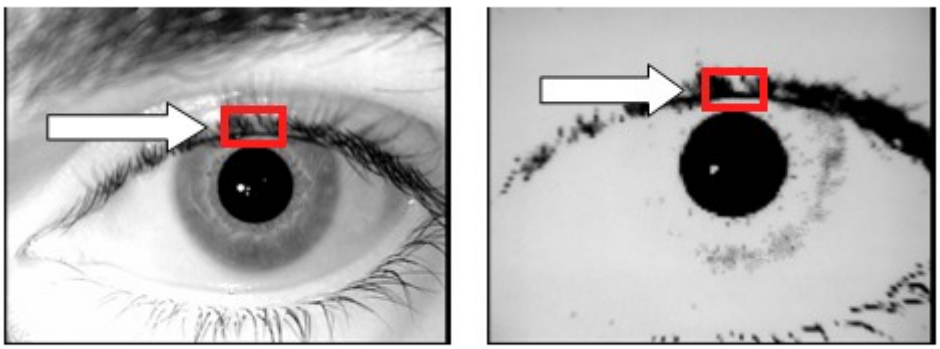


Figura 20. Región de interés usada para estimar el MCI3

Con esta medida podríamos entrar en la misma disyuntiva que la medida MCI5, de las medidas agrupadas en parámetros de movimiento, si deberían ser analizadas las imágenes por parejas o no ya que para esta medida es necesaria una segmentación previa y se supone deberían poseer ambas las mismas medidas y posiciones de iris y pupila. No obstante, al igual que se comentó anteriormente el análisis debe ser individual, incluso el error en el segmentador puede ser considerado como una ayuda para la detección de muestras sintéticas.

- **Relaciones de distribución de frecuencias 1 (MCI6-12)** [9]**:** Familia de diferentes combinaciones (suma, resta, multiplicación o división) de tres parámetros diferentes que consideran respectivamente la potencia de bajas (F1), medias (F2) y altas (F3) frecuencias (calculadas de acuerdo al espectro de la transformada de Fourier en dos dimensiones) de dos regiones locales de la imagen del ojo. El proceso se muestra en la Figura 21.

  Pese a estar incluidos en la clase de oclusión, o de enfoque estas medidas también podían ser clasificadas como de movimiento debido a su carácter de análisis de frecuencias.

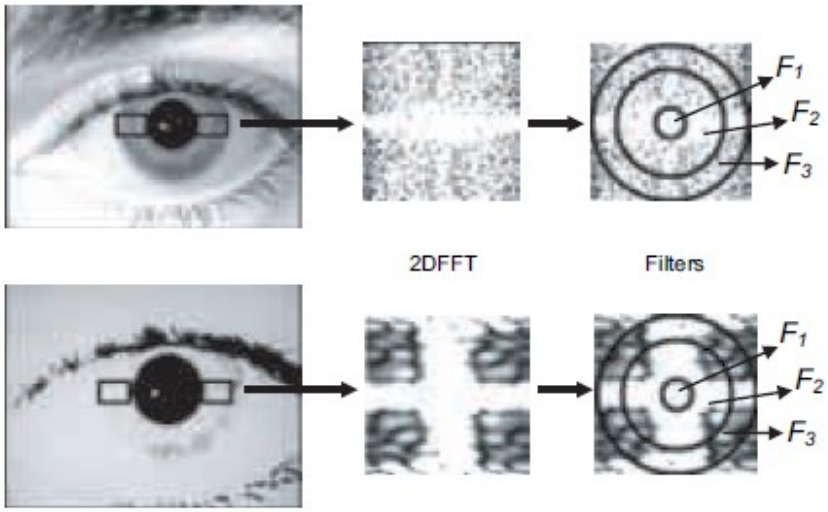


Figura 21. Proceso general de obtención de F1,F2 y F3 en MCI6-12.

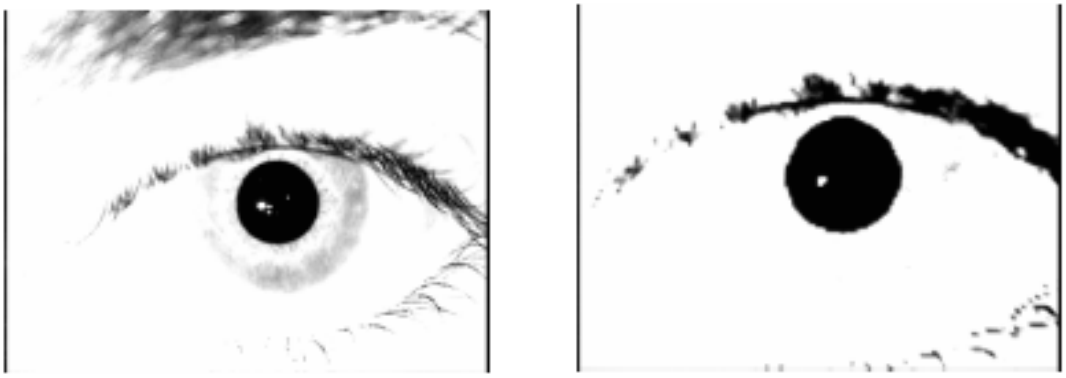
Unas de las combinaciones implementadas son las propuestas de los investigadores [9] aparecen en las dos primeras posiciones de la tabla 2, el resto de combinaciones son propuestas originales de este proyecto:

Medida de calidad	Combinación de F1, F2 y F3
MCI6 [9]	F1 + F2 + F3
MCI7 [9]	$\frac{F2}{F1+F3}$
MCI8	F3
MCI9	F2
MCI10	F1

MCI11	$\frac{\mathrm{F1} + \mathrm{F2}}{F3}$
MCI12	$\frac{F1 \times F2}{F3}$

Tabla 2. Medidas implementadas como combinación de F1, F2 y F3

- **Relaciones de distribución de frecuencias 2 (MCI17)** [11]**:** Similar a los anteriores, pero en este caso el iris se divide en múltiples regiones de frecuencia y el espectro se calcula usando la 2DCWT (2D Continuous Wavelet Transform).

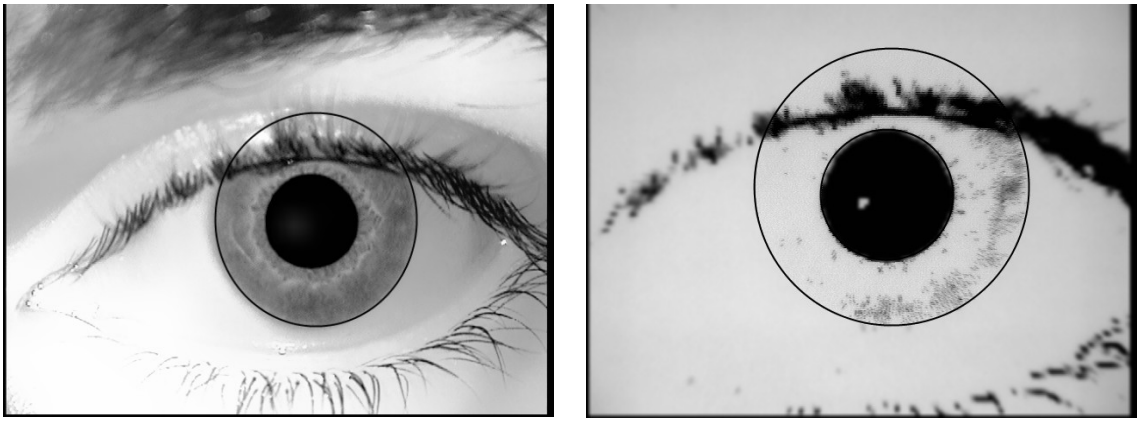


Real Sintético

Figura 22.Imágenes en el operador MCI17.

Tal como se aprecia en la figura 22, el operador CWT hace que sea muy difícil encontrar el iris en la imagen falsa. El operador anula las zonas claras en la escala de grises manteniendo sólo visibles las zonas con valores oscuros.

- **Relación entre iris e imagen (MCI19)** [29]**:** calcula la relación entre el área del iris segmentado y el resto de la imagen.



Real Sintético

Figura 23. Imágenes para el operador MCI19.

Como se aprecia en la figura 23, el operador usa la zona de la banda del iris para hacer el cálculo, en el ojo falso (la banda depende de la segmentación previa).

- **Binarización (MCI21)** [17]**:** estima el área no ocluida por párpados, pestañas y otros elementos haciendo una binarización de los píxeles de la imagen.

  Al tratarse de una técnica de medida de oclusión mediante binarización de las imágenes para detectar los cambios bruscos de grises, la binarización depende mucho del contraste de la imagen, podemos intuir que el hecho de realizar una captura (aunque sea de altísima calidad) de una imagen que a su vez es una reproducción (incluso de alta calidad) hace que la imagen resultante posea menor calidad de contraste y definición que la original. Este punto es el que puede ser clave para la identificación de las muestras sintéticas (definiendo sintéticas como imágenes impresas en alta resolución en este proyecto).

5.2.4 OTROS PARÁMETROS

En esta categoría están incluidas aquellas características que miden diferentes características del iris diferentes a las consideradas anteriormente en las otras clases. En particular dos indicadores de calidad estudian el contraste y la dilatación de la pupila.

- **Contraste global (MCI14)** [10]**:** para imágenes con escalas de 256 niveles, los valores próximos a 128 son consideradas como mejor zona de contraste. Los píxeles con valores muy altos o muy bajos son cambiados por valor 0 para así tener una escala normalizada entre 0 y 25, asignando los valores de 1 al 25 a los píxeles con valores próximos a 128. La función de transformación se muestra en la figura 24

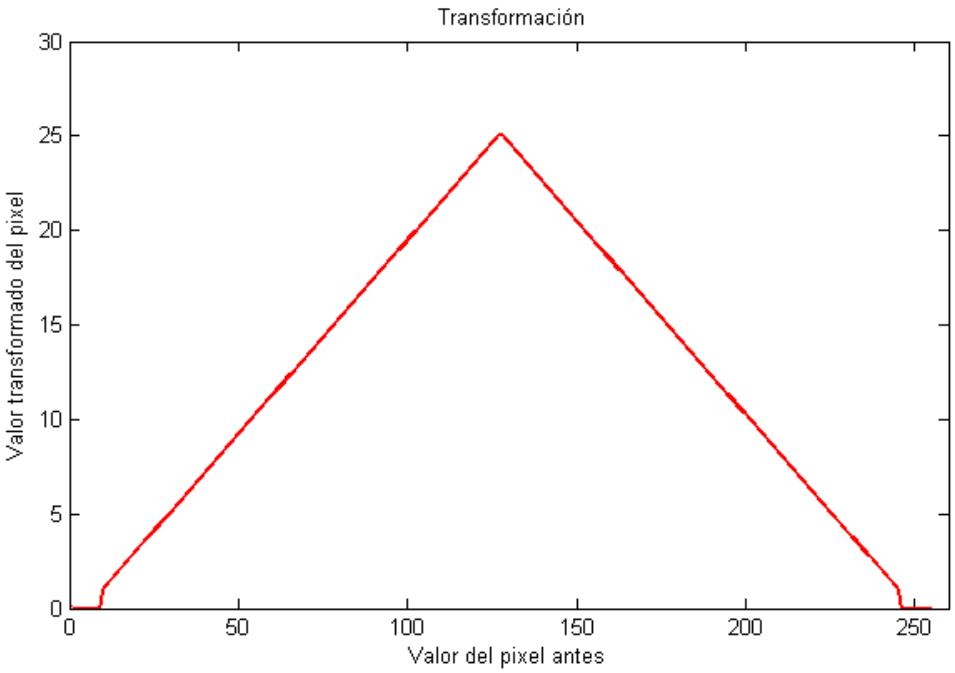
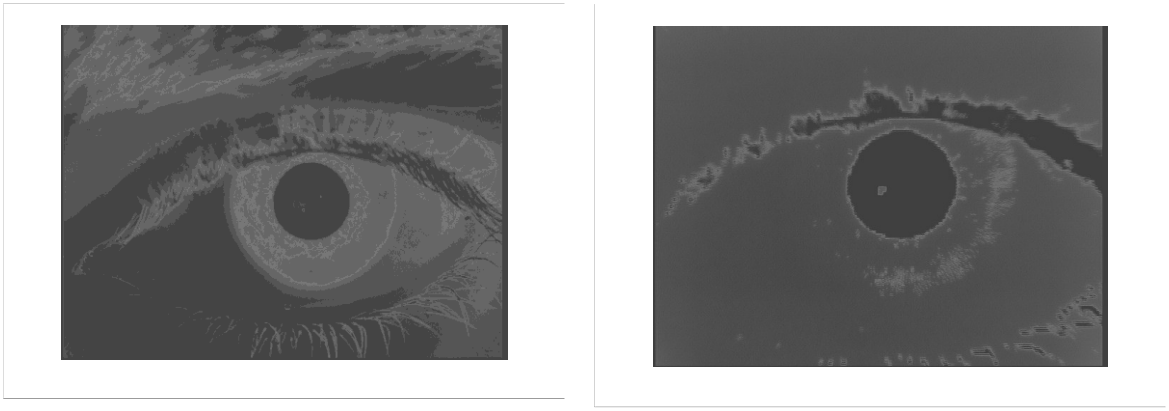


Figura 24. Transformación utilizada en el algoritmo de la medida MCI14



Real Sintético

Figura 25. Imágenes tratadas con Contraste global MCI14.

En la figura 25 Observamos el cambio de contraste y la diferencia entre un ojo real y uno sintético. Las imágenes han sido modificadas (aumentando el brillo y contraste) para exponerlas en esta memoria y poder apreciar mejor la diferencia entre ambos ojos.

- **Contraste local (MCI13):** nueva propuesta de medida de calidad para el trabajo, inspirada en una medida de calidad [10] para la obtención de oclusión.

  La región cuadrada que envuelve el iris y la pupila es dividida en celdas de 10x10 píxeles generando una rejilla de celdas.

  A cada celda es asignada por un valor que corresponde a la potencia de sus frecuencias medias.

  El valor de medida final se calcula haciendo la media de los valores de las celdas pero usando sólo aquellas celdas cuyos valores estén entre 20 y 60. Esta suma se divide entre el número total de las celdas para obtener la medida.
  El proceso se puede ver gráficamente en la figura 26:

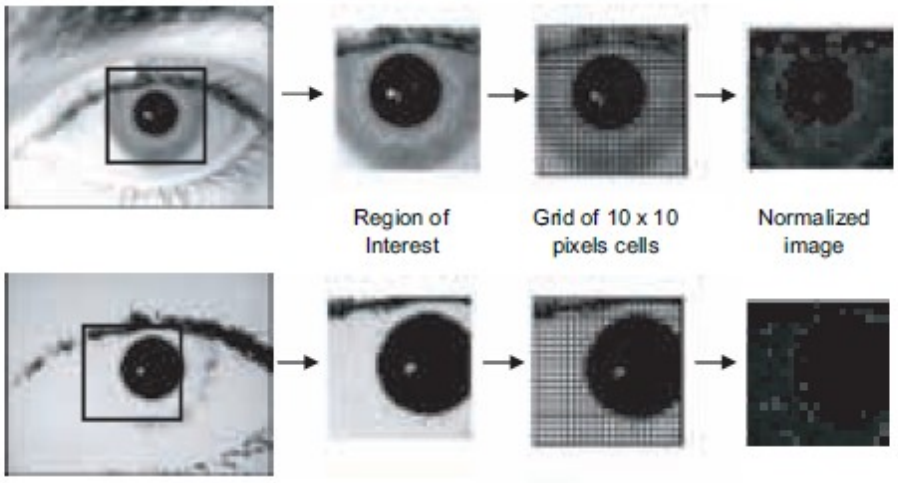


Figura 26. Proceso general seguido para calcular el MCI13 para un ojo real (arriba) y uno sintético (abajo)

Si analizamos paso a paso el proceso podemos, ya en el análisis con las dos imágenes de prueba, ver diferencias detectables a primera vista, debido al segmentador (paso previo a la medida de calidad) ya en la primera fase el área seleccionada para la imagen falsa contiene sólo parte del iris y no el total (como sí ocurre en la imagen real). Además si analizamos el final del proceso observamos muchos más cambios de grises en la imagen real.

• **Dilatación de la pupila (MCI22)** [17]**:** calcula la relación entre los radios de pupila e iris:

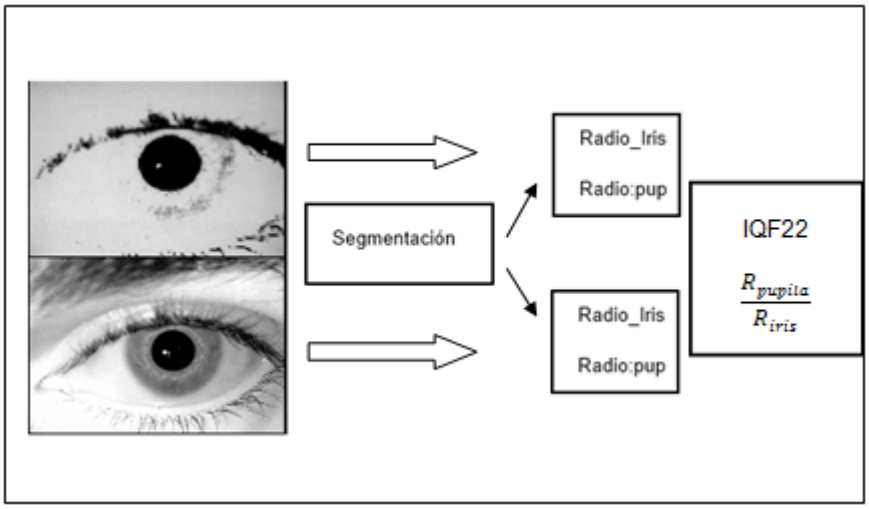


Figura 27. Proceso de obtención del factor MCI22

- **Otras medidas:** para este proyecto fueron implementadas otras 4 medidas que no han sido descritas ya que fueron retiradas del conjunto de medidas por causar problemas en el algoritmo de clasificación debido a las distribuciones de valores que tomaban.

5.3 SELECCIÓN DE CARACTERÍSTICAS Y CLASIFICADOR

Debido a la multidimensionalidad del método, es posible que los mejores resultados de clasificación no obtengan utilizando el conjunto de las 22 medidas implementadas, (descritas en el apartado 5.2), pero sí un subconjunto de ellas.

Al tener 22 medidas el combinarlas todas en subgrupos de 1 hasta 22 nos daría una cantidad de 2^{22}-1 experimentos, una cantidad inviable como para plantearnos hacer una búsqueda exhaustiva del subconjunto óptimo. Por esta razón se utilizó el algoritmo adaptado de Pudil [27] de selección de características Sequential Floating Feature Selection (SFFS) para obtener un error de clasificación mínimo.

Este algoritmo ha sido probado previamente y ha demostrado buenos resultados en comparación con otras técnicas de selección de características [19]. Consiste en una búsqueda de óptimos por iteraciones. En cada iteración el algoritmo basa la elección del siguiente subconjunto, en los resultados de subconjuntos anteriores (para nuestro caso la función de optimización es el error medio de clasificación producido).

Para la clasificación de las imágenes en Original y Sintético a partir de a los subgrupos de factores de calidad, se ha usado un clasificador estándar cuadrático (clasifica las muestras en función de la distancia cuadrática al centroide de cada una de las clases en las que se tendría que clasificar cada muestra), que devuelve la probabilidad (de 0 a 1) de pertenecer a cada unas de las clases.

Para la obtención del Error Medio de Clasificación (EMC) se utilizó la información del clasificador, estimando los errores de Falso Sintético (FSR) y Falso Original (FOR) y definiendo el EMC como el punto de cruce de las gráficas FSR y FOR .

En la figura 28 podemos observar las curvas FRR y FOR y el punto de cruce (EMC), para una de las medidas implementadas (IQF: Iris Quality Feature).

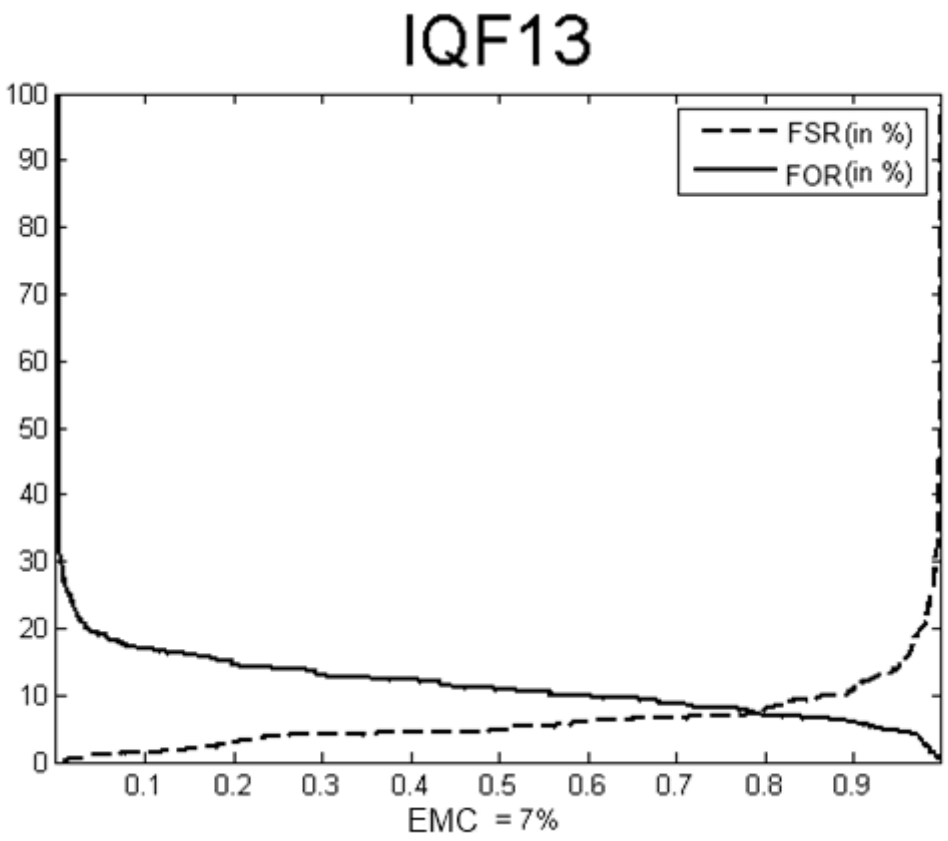


Figura 28. Curvas Falso Sintético (FSR) y Falso Original (FOR) para la obtención del Error Medio de Clasificación (EMC) en una de las medidas de calidad del algoritmo

6. BASES DE DATOS Y PROTOCOLO EXPERIMENTAL

La base de datos utilizada en los experimentos incluye imágenes de iris verdaderos y falsos de 50 usuarios de la base de datos de referencia BioSec [18]. Las muestras falsas fueron adquiridas después de un proceso de tres pasos [12]:

i) En primer lugar las imágenes originales fueron procesadas para mejorar la calidad final de los iris falsos.

ii) Posteriormente fueron impresas con una impresora comercial de alta calidad.

iii) Por último las imágenes impresas se presentaron al sensor de iris con el fin de obtener la imagen falsa.

La base de datos de iris falsos sigue la misma estructura que la base de datos original BioSec, por lo tanto, los datos utilizados en los experimentos hacen un total de:

50 usuarios * 2 ojos * 4 imágenes * 2 * sesiones = 800 imágenes falsas del iris y sus muestras originales correspondientes.

La adquisición de las muestras reales y falsas se llevó a cabo utilizando el sensor LG IrisAccess EOU3000. En la figura 29 se muestran algunas imágenes del iris típicas de iris verdaderos y falsos que se pueden encontrar en las bases de datos utilizadas.

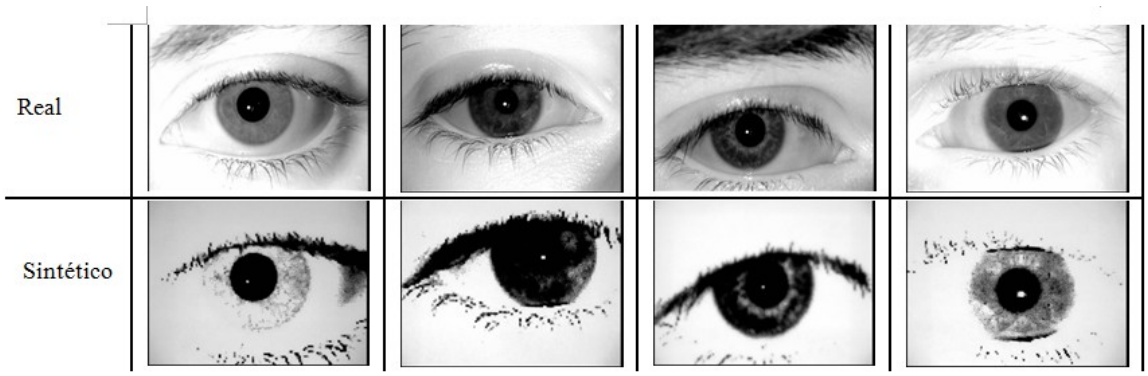


Figura 29. Ejemplos de imágenes de las bases de datos real y falsa

Como se puede observar en la figura 30, para los experimentos la base de datos se divide en un conjunto de entrenamiento (que comprende 200 imágenes reales y otras 200 muestras falsas), donde se llevan a cabo el proceso de selección de características y el entrenamiento de clasificadores, y un conjunto de prueba totalmente independientes (con las restantes 600 muestras reales y 600 falsas) para evaluar el rendimiento del sistema de detección de vida propuesto.

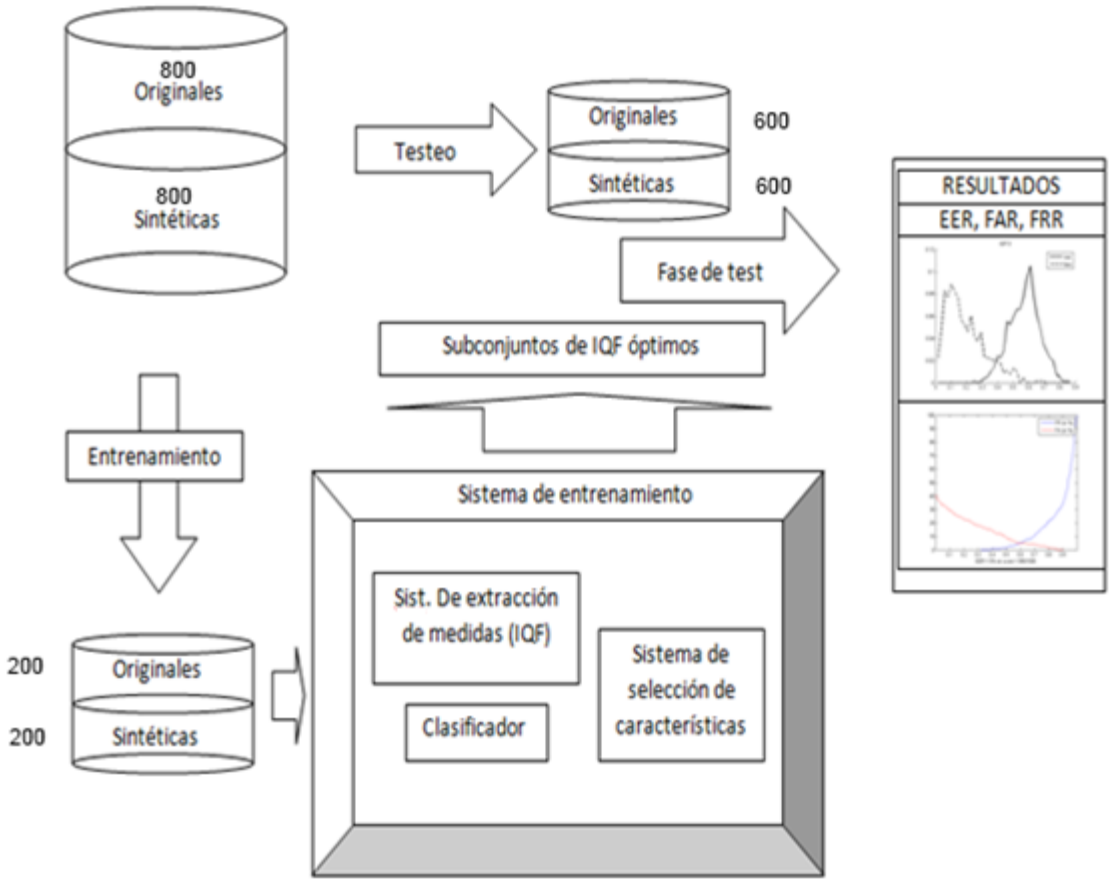


Figura 30. División de la base de datos.

6.1 PROTOCOLO EXPERIMENTAL

En la parte de experimentos, se realizaron 3 fases bien diferenciadas:

i) **Fase de diseño:** Se observó después de la implementación de cada medida individual el comportamiento de los conjuntos de imágenes (original y falso) mediante el uso de histogramas. Así podríamos evaluar aproximadamente la capacidad discriminativa de las medidas.
Posteriormente se realizó la división de la base de datos, como se muestra en la figura 30, para realizar la segunda y tercera fase de los experimentos (entrenamiento y test).

ii) **Fase de Entrenamiento:** Se midió la capacidad de detección de las medidas implementadas tanto individualmente como en grupos. Para medir la capacidad de detección valoramos el $EMC_{entrenamiento}$ (Error Medio de Clasificación en

entrenamiento) y utilizamos el algoritmo SFFS de Pudil, para la búsqueda de los conjuntos de medidas que hiciesen mínimo ese valor.
Una vez obtenidas las mejores combinaciones, entrenamos el clasificador con todas las muestras de esta fase, para en la siguiente fase pasar a clasificar las imágenes de test en función de las imágenes de entrenamiento.

iii) **Fase de Test:** Se obtuvieron los resultados definitivos del sistema enfrentando las imágenes de test a la configuración llevada a cabo en la fase de entrenamiento (tanto en el clasificador como las medidas a utilizar por ser mas discriminativas) observando la capacidad de detección de los mejores subconjuntos extrayendo el EMC_{test} (Error Medio de Clasificación en la fase de test) enfrentando la base de datos de test a la configuración de entrenamiento y así independizando los resultados.

Una vez obtenidos los resultados de las tres fases de experimentos, procedimos a comparar resultados, viendo concordancia y evaluando de las posibles diferencias entre los resultados en las fases de entrenamiento y de testeo.

7.RESULTADOS

Los objetivos principales marcados en la fase experimental son:

1. Evaluar individualmente el poder discriminativo entre imágenes reales y sintéticas de las medidas implementadas (fase de diseño).
2. Encontrar el mejor subconjunto de los parámetros implementados que nos permitan alcanzar la mejor tasa de reconocimiento en la detección de vida (fase de entrenamiento).
3. Evaluar de forma transparente y objetiva el rendimiento final del sistema de detección de vida basado en medidas de calidad que se ha desarrollado en el presente proyecto (fase de test).

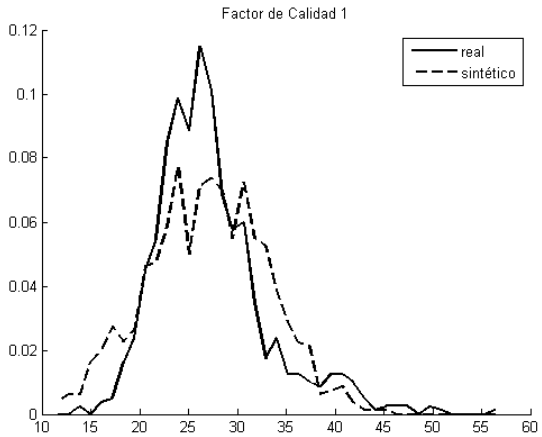
Para la obtención de estos resultados se siguió el protocolo mostrado en el apartado 6.1 de esta memoria.

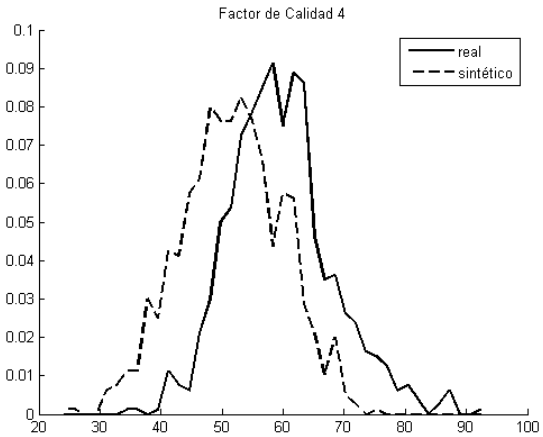
A continuación procedemos a mostrar los resultados siguiendo las fases definidas en el protocolo experimental:

7.1. FASE DE DISEÑO

Extrajimos los histogramas de las imágenes reales y sintéticas para cada una de las medidas y evaluamos una por una sus posibilidades de ser más o menos discriminativas para la detección de vida:

a) Medidas de Enfoque:





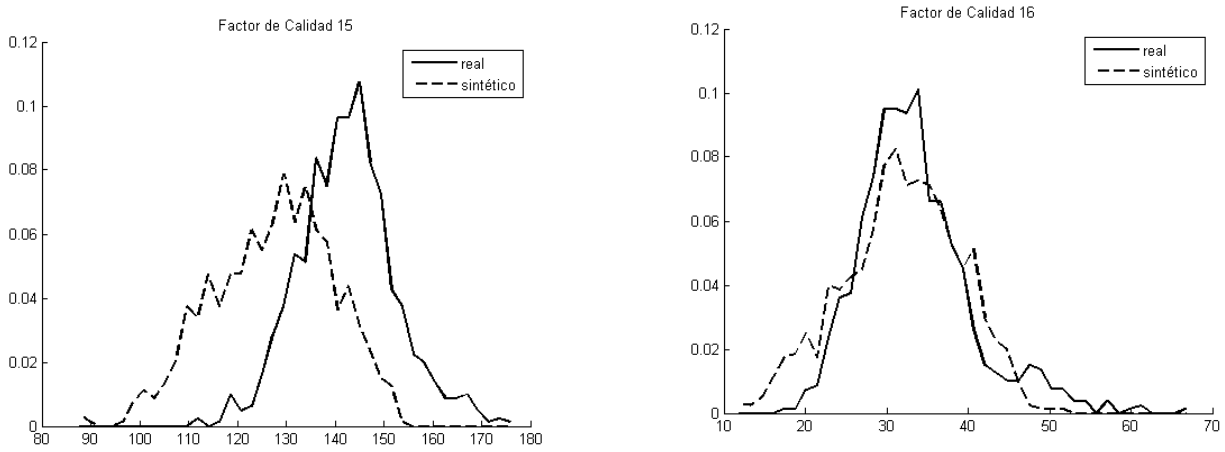
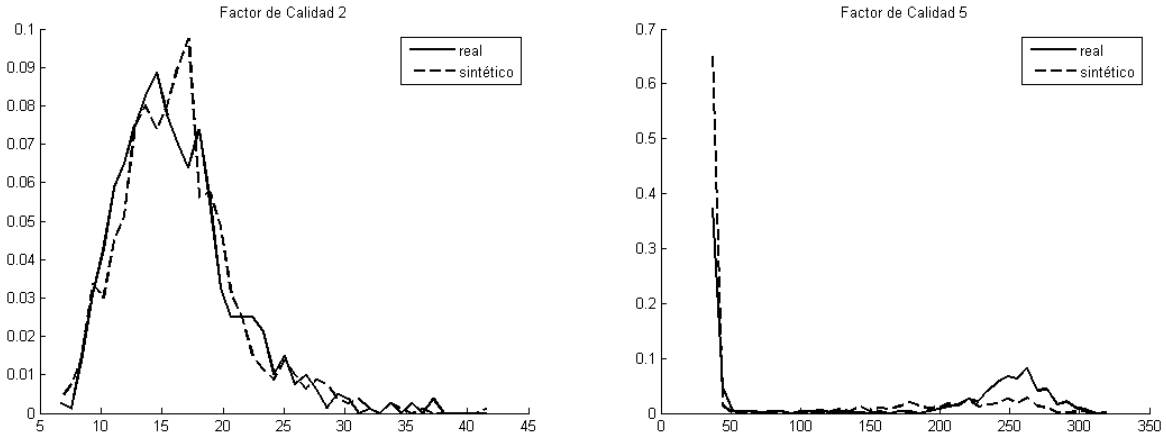


Figura 31. Histogramas de las medidas de calidad de Enfoque

Tal como se observa en la figura 31 las medidas de calidad 4 y 15 tienden a ser mas discriminativas entre imágenes reales y sintéticas. Las distribuciones de las imágenes reales están más separadas que las de las medidas 1 y 16.

b) Medidas de Movimiento:



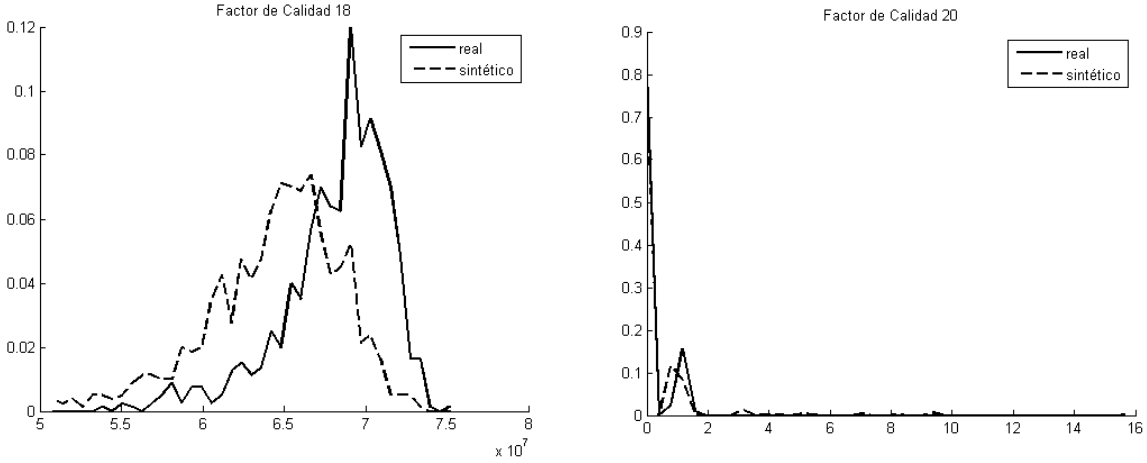
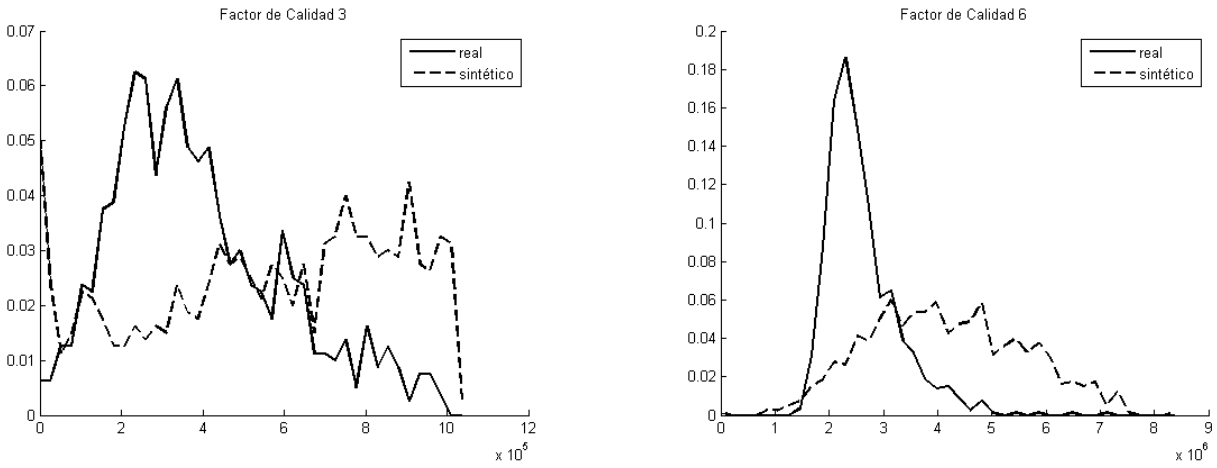


Figura 32. Histogramas par a las medidas de calidad de movimiento

Tal como se observa en los histogramas de la figura 32, se puede afirmar que las medidas de movimiento, implementadas para este proyecto, no poseen gran capacidad discriminativa. No obstante en combinación con otras medidas más discriminativas sí podrían ayudar a obtener un algoritmos más robusto debido a la multidimensionalidad del método que buscamos.

c) Medidas de Oclusión:



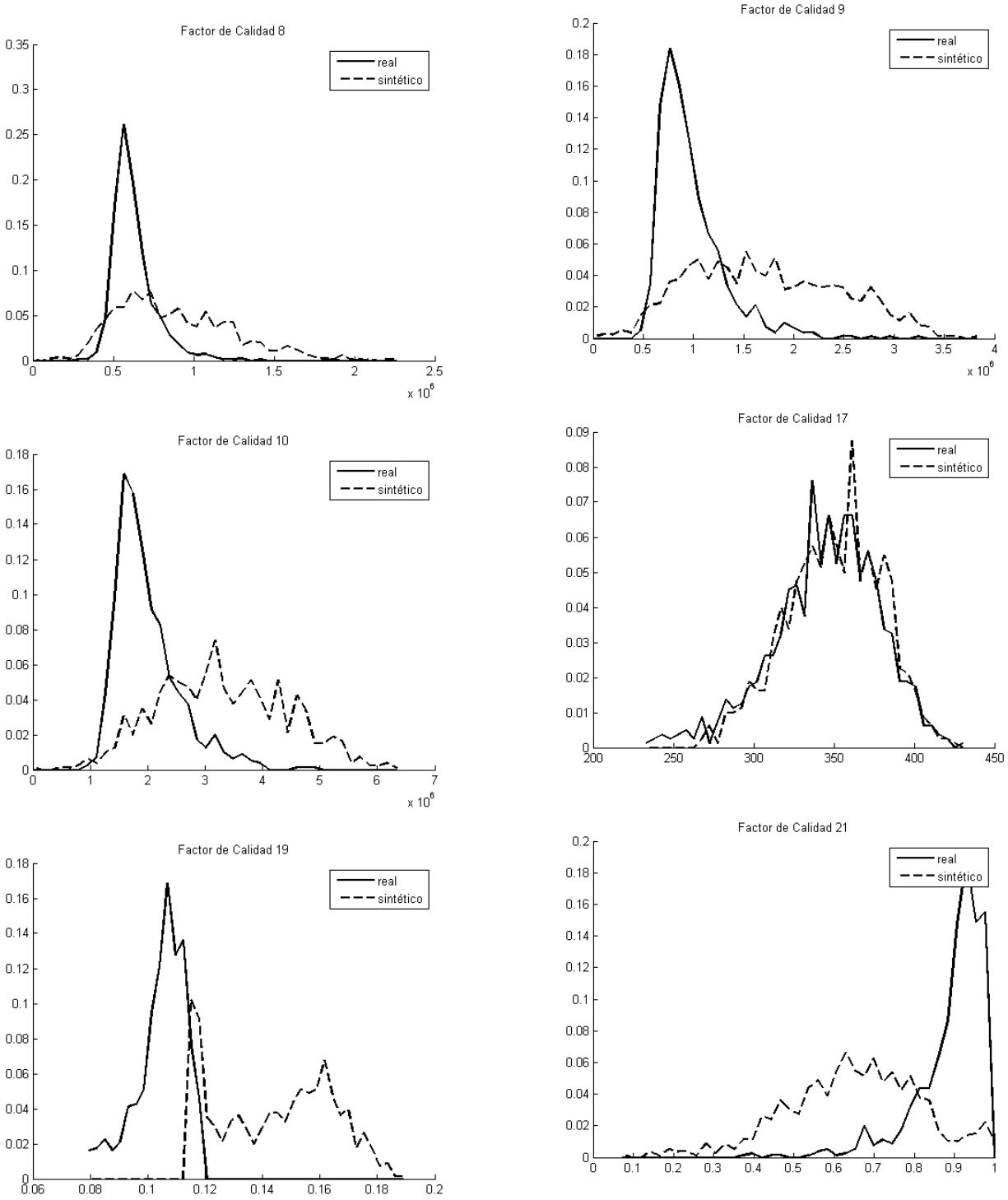


Figura 33. Histogramas pertenecientes a las medidas de calidad de las medidas de calidad de oclusión

En la figura 33 se muestra el comportamiento de las medidas de calidad de oclusión. Al observar las gráficas se puede prever la alta capacidad discriminativa el factor de calidad 19 (MCI19), de la medida 21. También podemos concluir algo muy similar como de la familia de medidas de calidad MCI6-12 (en las imágenes aparecen solo MCI6-10, por ser las más representativas). En cambio no podemos decir lo mismo de la 17 que posee un

histograma con distribuciones muy solapadas o de la medida 3, cuya distribución de imágenes sintéticas aproxima su comportamiento a una distribución uniforme.

d) Otras medias de calidad:

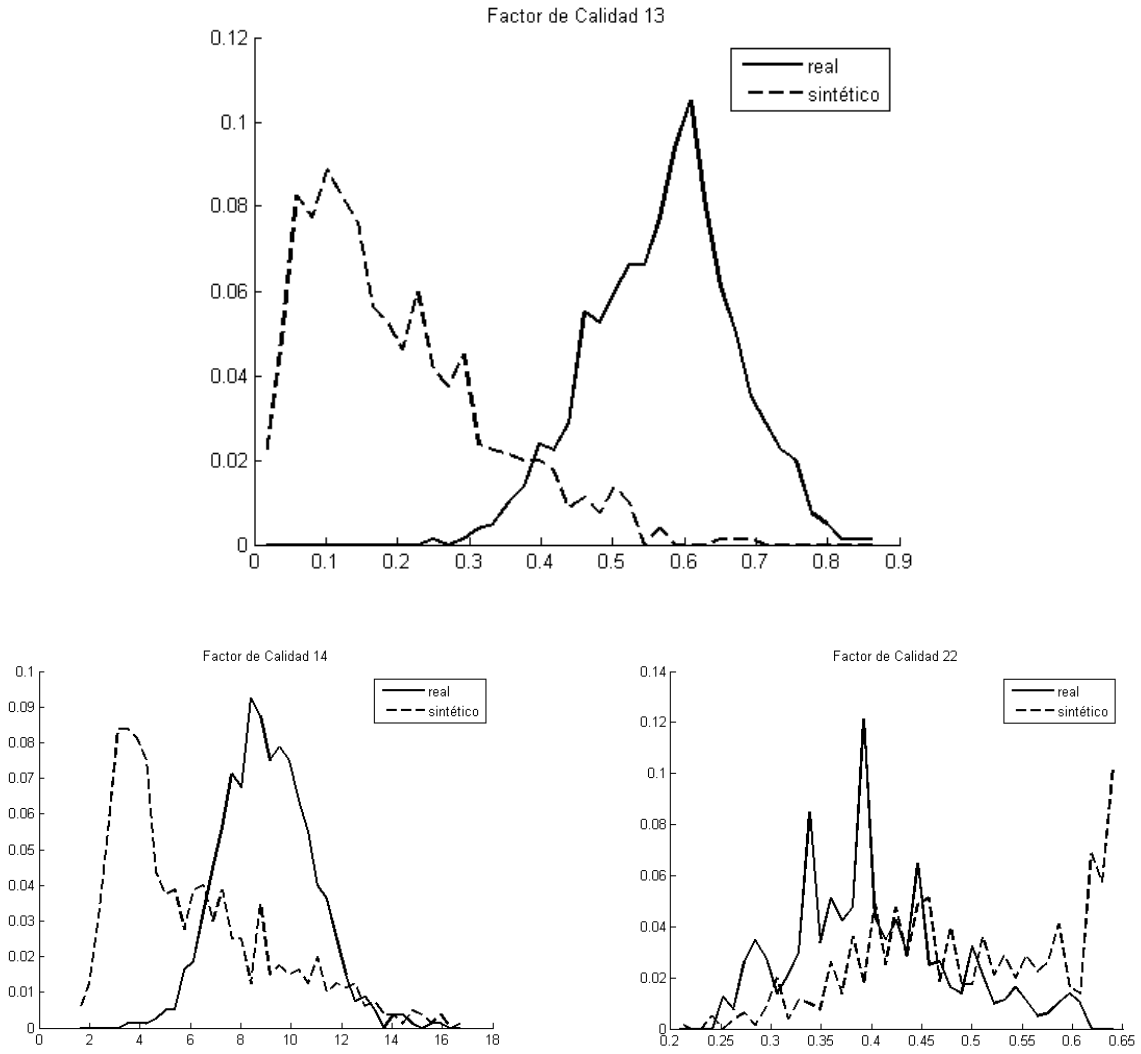


Figura 34. Histogramas de las medidas de calidad pertenecientes al grupo de otras medidas de calidad

En este último grupo de medidas, podemos apreciar gracias a la figura 34 dos medidas (MCI13 y MCI14) que previsiblemente serán también de un grado alto de discriminación debido al bajo solapamiento de las distribuciones de las imágenes reales y sintéticas en sus histogramas. No podemos decir los mismo de la medida de calidad 22 debido al alto grado de solapamiento de las distribuciones en su histograma.

7.2 FASES DE ENTRENAMIENTO Y TEST

Una vez extraídos los histogramas de las medidas de calidad dividimos la base de datos y procedimos a obtener resultados medibles mediante valores, en este caso utilizamos el EMC.
Comenzamos con la búsqueda de los mejores subconjuntos de medidas (aquellos que obtuviesen mínimo EMC) utilizando el algoritmo SFFS.

A la salida de la fase de entrenamiento obtuvimos los resultados que se pueden observar en la tabla 3. Una vez que el mínimo EMC es alcanzado, utilizamos los mejores subconjuntos de medidas de calidad para clasificar las imágenes de test (que durante todo el desarrollo del proyecto han sido mantenidas separadas de las muestras del conjunto de entrenamiento) para obtener resultados totalmente imparciales sobre la capacidad discriminativa del sistema.

En la tabla 3 también indicamos los resultados de clasificación del proyecto. Por claridad, sólo se muestran los mejores subconjuntos de características en el entrenamiento. Se muestran los valores de error medio de clasificación para el conjunto de entrenamiento (enfrentando 200 imágenes a otras 200 y viceversa) y para el conjunto de test (enfrentando las 1200 imágenes de test al algoritmo entrenado con las 400 de entrenamiento).

Orden	Subconjunto	Clase	$EMC_{entrenamiento}$ (%)	EMC_{test} (%)
1	MCI6	Oclusión	19,25	24,00
	MCI10	Oclusión	19,25	20,87
	MCI11	Oclusión	18,50	22,50
	MCI13	Contraste	5,75	7,37
	MCI19	Oclusión	4,25	10,50
	MCI21	Oclusión	14,75	14,62
2	MCI19 + MCI4	Oclusión + enfoque	2,25	5
	MCI19 + MCI13	Oclusión + contraste	0,25	3
	MCI19 + MCI14	Oclusión + contraste	2,75	6,50
	MCI19 + MCI15	Oclusión + enfoque	2,50	4,75
	MCI19 + MCI21	Oclusión + Oclusión	4,00	5,37
	MCI19 + MCI22	Oclusión + dilatación	0,00	0,00
3	MCI19 + MCI22 + MCI13	Ocl+dilat+ contras.	0,00	0,00
4	MCI19 + MCI22 + MCI13+…	Ocl + dilat+ contras.+…	0,00	0,00

Tabla 3.Resultados de clasificación para los mejores subconjuntos de características.

Se pueden sacar varias conclusiones de los resultados mostrados en la Tabla 3:

i) El método propuesto presenta un gran potencial como nuevo método para prevenir ataques directo, obteniendo un 100% de acierto clasificando correctamente las muestras de nuestra base de datos.

ii) Para las imágenes falsas usadas en el experimento (imágenes de alta calidad impresas) las características de oclusión parecen presentar el mejor comportamiento individual para la detección de vida.

iii) Cuando varias características son combinadas el mejor comportamiento es debido a la complementariedad de los parámetros midiendo diferentes características, lo que le hace al sistema ser más robusto (p.e. el primer 0%en errores se obtiene al combinar un parámetro de oclusión con otro de dilatación).

iv) El comportamiento similar de los resultados en entrenamiento y test nos indican que los resultados no son dependientes de las muestras utilizadas en ambos subconjuntos e invitan a pensar que estos buenos resultados se puedan mantener con otras bases de datos.

8.CONCLUSIONES Y TRABAJO FUTURO

En esta memoria se presenta un novedoso sistema de detección de vida para imágenes de iris, basado en medidas de calidad.

El método ha sido testado con una base de datos que comprende 1600 imágenes de ojos reales y copias de los mismo.

Se obtuvo un 100% de acierto en la clasificación de las imágenes (real o sintético). Con esto se prueba su potencial como una contramedida para prevenir ataques directos al sensor.

Además se han extraído diferentes conclusiones de acuerdo al potencial de cada tipo de medida implementada y la mejor forma de combinarlas para la detección de vida:

- Para los datos analizados las medidas de calidad que muestran un mayor poder discriminativo son las de oclusión.
- Los parámetros que miden características de calidad complementarias son más efectivos a la hora de implementar un sistema de detección de vida.
- La consistencia de los resultados obtenidos entre las fases de entrenamiento y test hacen pensar que el método propuesto alcanzará buenos resultados con independencia de los datos utilizados.

Las soluciones a la detección de vida, como la que se presenta en este trabajo son de gran importancia en el campo de la biometría ya que ayudan a prevenir ataques directos (aquellos llevados a cabo con reproducciones sintéticas, de gran dificultad para ser detectados), aumentando el nivel de seguridad ofrecido al usuario.

8.2 TRABAJO FUTURO.

Debido a la gran cantidad subgrupos de medidas de calidad que han conseguido clasificar todas las muestras correctamente, se plantea en el futuro buscar dentro de esos óptimos una combinación mejor que el resto. Para ello nos planteamos calcular la distancia entre las distribuciones de imágenes reales y sintéticas que se forman en el espacio n-dimensional para los subgrupos de n-características. Cuanto más separadas estén, más robusto será el algoritmo.

Otra medida que nos permita optimizar el método será aquella que tenga en cuenta el rendimiento necesario de procesador, ya que algunas de las medidas aquí implementadas requieren un tiempo elevado de procesamiento (entorno a la decena de segundos por cada imagen).Sería interesante estudiar estos tiempos de procesado y buscar el subconjunto de

menor tiempo de cálculo (a menor número de características, mas rápido será) y que tenga una separación mayor entre sus distribuciones.

Debido a la limitación de la base de datos, no se ha podido comprobar el funcionamiento del algoritmo con diferentes tipos de falsificaciones de iris como son vídeos, lentes de contacto, ojos sintéticos…(presentados en la sección 4.1). Sería muy interesante poder contrastar el algoritmo con otras bases de datos mayores y con mayor diversidad de tipos de ataques directos.

REFERENCIAS

[1]. Matsumoto, T., 2004. "Artificial irises: importance of vulnerability analysis." In: Proc. ABW.

[2]. Zuo, J., Schmid, N. A., et al., 2007. "On generation and analysis of synthetic iris images". IEEE Trans. IFS 2, 77-90.

[3]. Pacut, A., Czajka, A., 2006. "Aliveness detection for iris biometrics". In: IEEE ICCST. pp. 122-129.

[4]. Seelen, U. C., 2005. "Countermeasures against iris spoofing with contact lenses". Presentation at BC Conference.

[5]. Wei, Z., Qiu, X., Sun, Z., Tan, T., 2008. "Counterfeit iris detection based on texture analysis." In: Proc.ICPR.

[6]. Z.Wei, T. Tan, et al. Robust and fast assessment of iris image quality. In Proc. IAPR ICB*, pages 464–471. Springer LNCS 3832, 2006. 3*

[7]. Kalka, N., Zuo, J., Schmid, N., and Cukic, B. 2002. "Image Quality Assessments for Iris Biometric." In: Proc. Annual Meeting of the Gesellschafi flit Classification, pp. 445-452.

[8]. Galbally, J. Nov, 2009. Tesis Doctoral "Vulnerabilities and attack protection in security system based on biometric recognition"

[9]. L. Ma, T. Tan, et al. Personal identification based on iris texture analysis. IEEE Trans. On Pattern Analysis and Machine Intelligence*, 25:1519–1533, 2003. 4*

[10]. Aditya Abhyankar, Stephanie Schuckers. 2009 "Iris quality assessment and bi-orthogonal wavelet based encoding for recognition". In: Pattern Recognition

[11]. Y. Chen, S. C. Dass, and A. K. Jain. Localized iris image quality using 2d wavelets. In Proc. IAPR ICB*, pages 373-381, 2006. 4*

[12]. V. Ruiz-Albacete, P. Tome-Gonzalez, et al. Direct attacks using fake images in iris verification. In Proc. BioID*, pages 181–190. Springer LNCS-5372, 2008. 1, 2, 5*

[13] F. Alonso-Fernandez, J. Fierrez, et al. A comparative study of fingerprint image quality estimation methods. IEEE Trans. on Information Forensics and Security*, 2(4):734–743, 2008. 1*

[14] K. Bowyer, K. Hollingsworth, and P. Flynn. Image understanding for iris biometrics: A survey. Computer vision and Image Understanding*, 110:281–307, 2007. 3*

[15] J. Daugman. How iris recognition works. IEEE Trans. On Circuits and Systems for Video Technology, *14:21–30, 2004.3*

[16] J. Daugman. Iris recognition and anti-spoofing countermeasures. In Proc. Int. Biometrics Conf. (IBC), 2004

[17] Y. Du, C. Belcher, et al. Feature correlation evaluation approach for iris feature quality measure. Signal Processing, *90:1176–1187, 2010. 4*

[18] J. Fierrez, J. Ortega-Garcia, et al. BioSec baseline corpus: A multimodal biometric database. Pattern Recognition, *40:1389–1392, 2007. 5*

[19] A. K. Jain and D. Zongker. Feature selection: evaluation, application, and small sample performance. IEEE Trans. on Pattern Analysis and Machine Intelligence, *19:153–158, 1997. 4*

[20] R. A. Jarvis. Focus optimization criteria for computer image processing. Microscope, *24:163–180, 1976. 3*

[21] N. Kalka, J. Zou, et al. Image quality assessment for iris biometric. In Proc. SPIE BTHI III, *volume 6202, pages 61020D1–61020D11, 2005. 3*

[22] M. Kanematsu, H. Takano, and K. Nakamura. Highly reliable liveness detection method for iris recognition. In Proc. SICE ICICIT, *pages 361–364, 2007. 1*

[23] E. C. Lee, K. R. Park, and J. Kim. Fake iris detection by using purkinje image. In Proc. IAPR ICB, *pages 397–403, 2006. 1*

[24] A. Lefohn, B. Budge, et al. An ocularists approach to human iris synthesis. IEEE Trans. On Computer *Graphics and Applications, 23:70–75, 2003. 1*

[25] M. Martinez-Diaz, J. Fierrez, et al. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. Pattern Recognition Letters. *To appear. 1*

[26] N. Poh, T. Bourlai, et al. Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms. IEEE Trans. on Information Forensicsand Security, *4:849–866, 2009. 1*

[27] P. Pudil, J. Novovicova, and J. Kittler. Flotating search methods in feature selection. Pattern Recognition Letters, *pages 1119–1125, 1994. 2, 4*

[28] U. C. von Seelen. Countermeasures against iris spoofing with contact lenses. Technical report, Iridian Tech., 2005. 1

[29] J. Zou and N. A. Schmid. Global and local quality measures for nir iris video. In Proc. IEEE WCVPR, *pages 120–125, 2009. 3, 4*

[30]Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. IEE Trans. Circuits Syst. Video Techn. 1(2): 125-143,2006.

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

[32]Leonard Flom and Aran Safir. Iris recognition systems, united states patent 4.641.349,1987

[33] Jhon Daugman Biometric personal identification systems based on iris analysis, United States panten 5.291.560, 1994

[34] 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

[35] Zhaofeng He, Tienu Tan, and Zhenan Sun. Iris localization via pulling and pushing. IN: ICPR '06: Proccedings of the 18th International Conference on Pattern Recognition, pages366-369,Whasington, DC, USA,2006 IEE Computer Society.

[36] Mihran Tucceryan. Momento-based texture segmentation. Pattern Recognition letters 15(7): 659-668, 1994

[37] Bori Toth, Ulf Cahn y Seelen Liveness Detection for Iris recognition 2005 In NIST Work Shop Biometrics and E-Autehentication over Open Networks, Gaithersburg (MD)

[38] Mark lane and Lisa Lordan "practical techiniques for defeating biometric devices", in: MSc. Security and Forensic Dublin City University

[39] X.HE, S. An y P. Shi, "Statistical Texture Analysis-Based Approach for Fake Iris Detection Using Support Vector Machines" in Institute of image processing and Pattern Recognition, Shangai Jiao Tong University, Shangai, 200240

[40] D1_12, NASK Iris recognition with aliveness detection, Project number IST- 2002-001766

[41] Schucker 2002 "Spoofing and anti-spoofing measures"

[42] Daugman 2006 liveness detection, Anti-spoofing "liveness Detection" Computer Laboratory to the University of Cambridge

[43] Z.Wei, X Qiu, Z. Sun and T. Tan. "Counterfeit Iris detection Based on texture Analysis" In Proc. IEEE Int.Conf. on Pattern Recognition (ICPR), 2008.

[44] X. He, Y Lu anda P. Shi "A new fake iris detection method" Chinese universities publication

[45] Lisa Thalheim, Jan Krissler, and Peter-Michael Ziegler Body Check: Biometric Access Protection Devices and their Programs Put to the Test.

[46] M. Lane and L. Lordan. Practical techniques for defeating biometric devices. Master Thesis, Dublin CityUniverstity, 2005.

[47]Marcos MArtinez-Diaz, J.Fierrez, J.Galbally, J.Ortega. "An evaluation of indirect attacks and countermeasures in fingerprint verification system". In: Pattern Recognition Letters 32 (2001), 1643-1651

[48]J.Galbally, C. McCool, J.Fierrez,S.Marcel "On the vulnerability of face verification systems to hill-climbing attacks" In: Patern Recognition 43(2010) 1027-1038.

[49] Andy Alder. "Sample Images can be Independently Restored from Face Recognition Templates" In: School of Information Technology and Engineering, University of Onawa, Ontario, Canada

[50] Christian Rathgeb and Andreas Uhl ." Attacking Iris Recognition: An Efficient Hill-Climbing Technique". In: 2010 International Conference on Pattern Recognition

PRESUPUESTO

1) Ejecución Material

- Compra de ordenador personal (Software incluido)..... 2.000 €
- Material de oficina ..... 150 €
- Total de ejecución material ..... 2.150 €

2) Beneficio Industrial

- 6 % sobre Ejecución Material ..... 129 €

3) Honorarios Proyecto

- 900 horas a 15 € / hora ..... 13500 €

4) Material fungible

- Gastos de impresión ..... 280 €
- Encuadernación ..... 200 €

5) Subtotal del presupuesto

- Subtotal Presupuesto ..... 16259 €

6) I.V.A. aplicable

- 18% Subtotal Presupuesto ..... 2926,62 €

7) Total presupuesto

- Total Presupuesto ..... 19185,62 €

Madrid, Septiembre de 2011

El Ingeniero Jefe de Proyecto

Fdo.: Jaime Ortiz López

Ingeniero Superior de Telecomunicación

PLIEGO DE CONDICIONES

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un **SISTEMA DE DETECCIÓN DE VIDA VÍA SOFTWARE EN IMÁGENES DE IRIS UTILIZANDO CRITERIOS DE CALIDAD**. 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% del presupuesto y la provisional del 2%.

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” y 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.

ANEXO I: PUBLICACIONES

El trabajo presentado en esta memoria y directamente derivado del Proyecto de Fin de Carrera ha dado lugar a dos artículos de investigación en conferencia internacional con revisión que se adjuntan en el presente anexo

- J.Ortiz-Lopez, J.Galbally, J.Fierrez, J.Ortega-García "Predicting Iris Vulnerability to Direct Attacks Based on Quality Related Features" In: Int.Carnahan Conf. on Security Technology (ICCST), Barcelona 2011 (accepted).

- J.,Galbally, J.Ortiz-Lopez, J.Fierrez and J.Ortega-García "Iris Liveness Detection Based on Quality Related Features" In: Int. Conference on Biometrics (ICB) New Delhi 2012(submitted)

Predicting Iris Vulnerability to Direct Attacks Based on Quality Related Features

Jaime Ortiz-Lopez, Javier Galbally, Julian Fierrez and Javier Ortega-Garcia
ATVS - Biometric Recognition Group
Universidad Autonoma de Madrid, EPS
C/ Francisco Tomas y Valiente, 11. 28049 Madrid. SPAIN
{*jaime.ortiz,javier.galbally,julian.fierrez,javier.ortega*}*@uam.es*

***Abstract*—A new vulnerability prediction scheme for direct attacks to iris recognition systems is presented. The objective of the novel technique, based on a 22 quality related parameterization, is to discriminate beforehand between real samples which are easy to spoof and those more resistant to this type of threat. The system is tested on a database comprising over 1,600 real and fake iris images proving to have a high discriminative power reaching an overall rate of 84% correctly classified real samples for the dataset considered. Furthermore, the detection method presented has the added advantage of needing just one iris image (the same used for verification) to decide its degree of robustness against spoofing attacks.**

***Keywords*-Security; Vulnerability; Iris recognition; Quality assessment;**

I. Introduction

Due to the fact that biometrics [1], as an automatic means of human recognition, constitutes a relatively novel field of research, most efforts undertaken by the different parties involved in the development of this technology (researchers, industry, evaluators, etc.) have been mainly (but not exclusively) directed to the improvement of its performance [2]. This has left partially uncovered other important aspects involved in the complex biometric recognition problem.

In particular, it has not been until recently when biometric security assessment has emerged in the biometric community as a primary field of research, as a consequence of the concern arisen after the classification of the vulnerability points presented in [3], and the different efficient attacking algorithms developed in order to compromise the security level given by biometric applications [4], [5].

These vulnerability studies have helped to improve the biometric technology by making public certain flaws and by encouraging the industry and researchers to look for solutions to the different threats [6], [7]. This way, the level of security and the convenience offered to the final user are increased.

External attacks which may compromise the security of biometric systems are commonly divided into two different groups, namely: *i) direct attacks*, carried out against the sensor using synthetic traits, such as printed iris images or gummy fingers [8], [9]; and *ii) indirect attacks*, carried out against one of the inner modules of the system [10], [11], and thus requiring some knowledge about the inner working of the system. In 2001, Ratha *et al.* made a more detailed analysis of the vulnerable points of biometric systems in [12], where 8 possible points of attack are identified. In Fig. 1, a generic iris recognition system is depicted, together with these 8 points of attack, where point 1 corresponds to the direct attacks, and the remaining seven points to the indirect attacks.

Within the studied vulnerabilities, special attention has been paid to direct attacks as they present the advantage over the indirect type of requiring less information about the system (e.g., features used, template format). Furthermore, as they are carried out outside the digital domain these attacks are more difficult to be detected as the digital protection mechanisms (e.g., digital signature, watermarking) are not valid to prevent them.

One of the main conclusions that may be drawn from previous studies on the security evaluation of biometric systems to direct attacks, is that not all biometric samples are equally robust to spoofing strategies, and that this resistance level is many times related to the biometric quality of the image [13]. Thus, it would be desirable in a biometric system to be able to detect beforehand those samples which are specially easy to be compromised with these spoofing techniques in order to adopt the necessary protection mechanisms (e.g., sample recapture, liveness detection methods, challenge-response approaches) which guarantee the same security level for all the users.

In the present work we concentrate our efforts in studying direct attacks against iris-based verification systems. In particular, we explore the potential of quality assessment (already considered in the literature for multimodal fusion [14], or score rejection [15]) to predict the level of robustness of a given iris sample against an eventual direct attack carried out with high quality printed images.

As state-of-the-art system for our study, we use a modified version of the Libor-Masek implementation [16], which is widely used in many iris related publications. Regarding the database used for our study, a new iris database has been created using iris images from 50 users of the BioSec baseline database [17]. The fake iris samples are obtained by acquiring high quality printed images with the LG IrisAccess EOU3000 sensor. The final dataset used in the experiments comprises 50 users $\times$ 2 eyes $\times$ 4 images $\times$ 2 sessions =

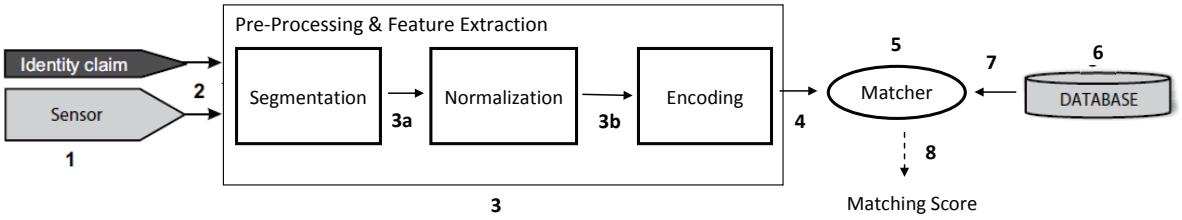


Figure 1. Architecture of an automated iris verification system. Possible attack points are numbered from 1 to 8.

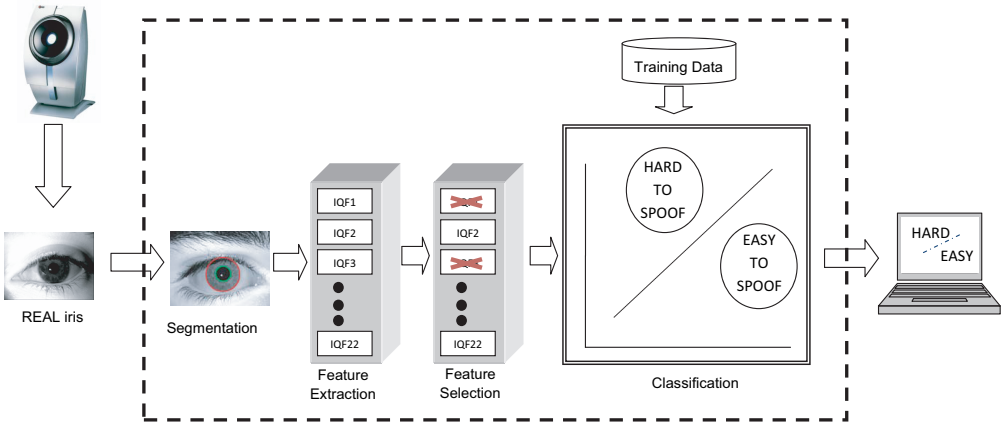


Figure 2. General diagram of the vulnerability prediction system presented in this work.

800 fake iris samples, and its corresponding real images.

The rest of the paper is structured as follows. A review of previous studies regarding the vulnerability of iris recognition systems to direct attacks is given in Sect. II. Sect. III describes the quality based method we have developed to predict the vulnerability degree of a certain iris sample. In Sect. IV the database and protocol used in the experiments is presented, and results are given in Sect. V. Conclusions are finally drawn in Sect. VI.

II. Related Works

One of the first efforts in the vulnerabilities study of iris verification systems to direct attacks was carried out in [5]. In that work an iris image of a legitimate user was printed with a high resolution inkjet printer to fraudulently access the system. The trick was only successful if the pupil in the image was cut out and the eye of the impostor placed behind the paper to give the impression to the system of a real eye. Only one commercial system was tested in the experiments showing high vulnerability to this type of attacks. It not only permitted the access with the fake iris, but also allowed the attacker to log on to the system using the iris picture.

Similar experiments in iris spoofing were described in [27]. Three different iris verification systems were tested, two portable and a hard-core device for gate control. Two different devices were used in the experiments to acquire the images for the fake irises, the camera embedded in the IrisPass-h system and a digital microscope with infrared lighting. As explained in Thalheim's experiments [5], the images were then printed using a high resolution inkjet printer and the pupil removed from the picture in order to place the impostor's eye behind the fake iris. All the systems tested were bypassed using the images captured with both acquisition devices.

Other works reporting iris spoofing have been published using again simple quality iris images [8], [28], printed contact lenses [7], [29], or even sophisticated multilayered 3D artificial irises [30].

III. Vulnerability Prediction System

The problem of iris vulnerability prediction to direct attacks can be seen as a two-class classification problem where a real iris image has to be assigned to one of two classes: easy or difficult to spoof. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image vulnerability given the extracted set of features. In the present work we propose a novel prediction system based on quality related measures.

A general diagram of prediction system presented in this work is shown in Fig. 2. Just one input is given to the system: the iris image to be classified (the same one used

Class	Features
Focus	*IQF1* [18], *IQF4* [19], *IQF15* [20], *IQF16* [18]
Motion	*IQF2* [18], *IQF5* [21], *IQF18* [22], *IQF20* [23]
Occlusion	*IQF3* [18], *IQF6-12* [24], *IQF17* [25], *IQF19* [23], *IQF21* [26]
Others	*IQF13* [20], *IQF14* [20], *IQF22* [26]

Table I
SUMMARY OF THE 22 QUALITY RELATED FEATURES IMPLEMENTED, CLASSIFIED ACCORDING TO THE IRIS CHARACTERISTIC MEASURED. THE REFERENCE TO THE WORKS WHERE THEY WERE FIRST PROPOSED IS ALSO GIVEN.

for verification). In the first step the iris is segmented from the background, for this purpose, a circular Hough transform is used in order to detect the iris and pupil boundaries as proposed in [8]. Once the useful information of the total image has been separated, twenty-two different quality measures are extracted which will serve as the feature vector that will be used in the classification. Prior to the classification step (where a standard quadratic classifier fitting the training data with multivariate normal densities has been used), the best performing features are selected using the Sequential Floating Feature Selection (SFFS) algorithm [31]. Once the final feature vector has been generated the iris is classified as easy/hard to spoof.

The parameterization used in the present work and applied to vulnerability detection was proposed in [32] for liveness detection and comprises twenty-two quality-based features adapted from different parameters described in the literature which measure one of the following properties:

- **Focus**. Intuitively, an image with good focus is a sharp image. Thus, defocus primarily attenuates high spatial frequencies, which means that almost all features estimating this property perform some measure of the high frequency content in the overall image or in the segmented iris region.
- **Motion**. This type of features try to estimate the image blur caused by motion (of the iris or of the sensor). The effect of motion is generally reflected on the directionality of the image, thus, these estimators are usually based on the computation of the preponderant directions within a given iris sample.
- **Occlusion**. These features try to detect those areas of the iris which are occluded by some external element such as the eyelids or the eyelashes. In this case different heterogeneous schemes have been proposed in the literature studying in general local characteristics of the iris image.
- **Other features**. In this category are included all those features measuring some different iris characteristic to those considered in the previous classes. In particular, the two quality indicators taken into account here will be the contrast (features *IQF13* and *IQF14*) and the pupil dilation (feature *IQF22*).

A summary of the different quality features used in this work and the characteristic that they measure (i.e., class to which they may be assigned) is given in Table I together with the reference to the original work where they were first proposed.

IV. IRIS VERIFICATION SYSTEM AND DATABASES

The vulnerability experiments are carried out on a modified version of the iris recognition system developed by L. Masek [1] [16], which is widely used in many iris related publications. As depicted in Fig. 1, the system comprises four different steps:

- **Segmentation**: the method proposed in [8] is followed: the system uses a circular Hough transform in order to detect the iris and pupil boundaries, which are modelled as two circles.
- **Normalization**: a technique based on Daugman's rubber sheet model [19] is used, mapping the segmented iris region into a 2D array.
- **Feature encoding**: the normalized iris pattern is convolved with 1D Log-Gabor wavelets. The encoding process produces a binary template of $20\times480 = 9,600$ bits and a corresponding noise mask that represents the eyelids areas.
- **Matching**: the inverse of the Hamming distance is used for matching. It is modified so that it incorporates the noise mask, using only the significant bits. A number of Hamming distance values are calculated from successive shifts [19], correcting this way for misalignments in the normalized iris pattern caused by rotational differences during imaging, being the lowest value finally taken.

For the experiments, the images that were not successfully segmented by the recognition system (3.04% of the 1,600 images available) were segmented manually, allowing us this way to use all of the available dataset. Furthermore, by doing this manual aided segmentation the system performance is optimistically biased and therefore harder to attack than in a practical situation (where the segmentation would be fully automatic).

In order to avoid biased results, two totally different datasets are used in the experiments:

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

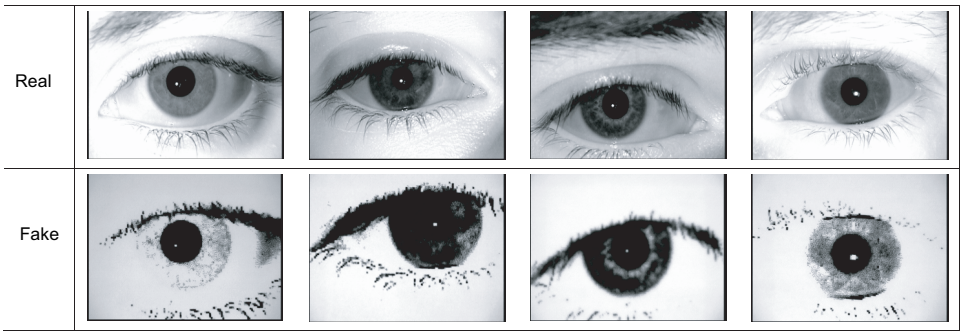


Figure 3. Typical real iris images and their corresponding fake samples that may be found in the database used in the experiments.

- **Performance Evaluation: Biosecure DS2** [33]. The iris subcorpus included in the Desktop Dataset of the BioSecure multimodal database [33] comprises four grey-scale images per eye from 210 users captured in two different sessions (two samples per session) and all captured with the Iris Access EOU3000 sensor from LG.
  This dataset is used to evaluate the performance of the iris verification system in order to set the threshold which separates easy to spoof real irises (those that produce scores higher than that threshold when compared to artificial iris images), from hard to spoof real samples (the generated scores when attacked with fake samples are lower than the threshold). Finally, the decision threshold was set to that corresponding to an operating point of FAR=0.01%, which represents a high security application according to [34].
- **Security Evaluation: FakeIris DB** [8]. This dataset comprises real and fake iris images of 50 users of the BioSec baseline database [17]. The fake samples were acquired following a three step process [8]: i) first original images were processed to improve the final quality of the fake irises, ii) then they were printed using a high-quality commercial printer, and last iii) the printed images were presented to the iris sensor in order to obtain the fake image.
  The fake iris database follows the same structure as the original BioSec database, therefore, the data used in the experiments comprises 50 users $\times$ 2 eyes $\times$ 4 images $\times$ 2 sessions $=$ 800 fake iris images and its corresponding original samples. The acquisition of both real and fake samples was carried out using the LG IrisAccess EOU3000 sensor. In Fig. 3 we show some typical real and fake iris images that may be found in the dataset.
  The real images of this database are classified into easy/hard to spoof samples according to the threshold computed using the iris subcorpus in Biosecure DS2. In order to perform this classification, the four fake images of a real iris are matched against their corresponding real sample. Then, the mean of the four scores is computed. If the averaged score is higher than the given threshold the real iris sample is assigned to the easy to spoof class, and to the hard to spoof class otherwise. This process leads to a 104/696 distribution of the real samples for the two classes: easy/hard to spoof.
  For the vulnerability prediction experiments, the real samples in the database are divided into a training set (comprising 348 vulnerable images and 52 robust samples) where the feature selection process and the classifier training are performed, and a totally independent test set (with the remaining 348 vulnerable and 52 robust images) to evaluate the performance of the proposed vulnerability detection approach.

V. Results

The first step in the experiments is to parameterize all the *real* images in the FakeIris DB according to the 22 feature set described in Sect. III. Once the parameterization has been completed the feature selection process is applied to the training set in order to find the optimal feature subsets for vulnerability prediction. For this purpose the classification performance of each of the optimal subsets is computed on the training set in terms of the Average Classification Error which is defined as ACE $=$ (FVR $+$ FRR)$/2$, where the FVR (False Vulnerable Rate) represents the percentage of robust (i.e., hard to spoof) fingerprints misclassified as vulnerable (i.e., easy to spoof), and the FRR (False Robust Rate) computes the percentage of vulnerable fingerprints assigned to the robust class.

Once the optimal subsets have been found and evaluated using the train set, their performance is finally assessed on the test set (which has no overlap with the training samples) in order to obtain totally unbiased results about the discriminant capabilities of the system. In Table II we summarize the results obtained in the classification process. For clarity, only the best feature subsets in the training phase are given. The performance results shown correspond to the classification threshold where FVR=FRR=ACE.

# features	Feature Subset	Class	ACE_{train} (%)	ACE_{test} (%)
1	*IQF6*	Occlusion	49.65	44.81
	IQF13	Contrast	49.54	43.84
	IQF14	Contrast	37.97	43.98
	IQF17	Occlusion	39.97	37.32
	IQF18	Motion	40.11	44.54
	IQF20	Motion	32.86	51.38
2	*IQF20 + IQF5*	Motion + motion	31.15	37.51
	IQF20 + IQF14	Motion + contrast	33.62	38.42
	IQF20 + IQF17	Motion + occlusion	34.26	36.81
	IQF20 + IQF18	Motion + motion	25.26	30.05
	IQF20 + IQF19	Motion + occlusion	29.78	31.14
	IQF20 + IQF22	Motion + dilation	33.63	34.92
3	*IQF20 + IQF18 + IQF4*	Mot. + mot. + focus	24.31	30.11
	IQF20 + IQF18 + IQF5	Mot. + mot. + motion	13.96	16.02
	IQF20 + IQF18 + IQF14	Mot. + mot. + contrast	26.51	31.28
	IQF20 + IQF18 + IQF17	Mot. + mot. + occlusion	23.01	35.75

Table II
CLASSIFICATION RESULTS FOR THE BEST FEATURE SUBSETS. ACE_{TRAIN} AND ACE_{TEST} REPRESENT RESPECTIVELY THE AVERAGE CLASSIFICATION ERROR IN THE TRAIN AND TEST SETS.

Several observations may be extracted from the results shown in Table II: i) the proposed system presents a relatively good discriminant power in order to distinguish between easy and hard to spoof samples (84% of correctly classified samples for the best configuration found) showing this way the feasibility of using quality related features for this purpose; ii) for the fake samples taken into account (high quality iris printed images) the motion features seem to present the best performance for vulnerability detection (the best result is obtained for a combination of three of these parameters); iii) the significant difference in performance between the train and the test set may indicate a certain dependence of the results to the data, so similar experiments should be carried out for different types of fake images.

VI. CONCLUSIONS

A novel vulnerability prediction system for spoofing attacks to iris recognition systems. The proposed method, based on a 22 feature set of quality related parameters, was tested on an iris database which comprises 1,600 real and fake images, where it reached a total 86% of correctly classified (robust/vulnerable) real samples, proving this way its feasibility as a strategy to prevent direct attacks to the sensor. Furthermore, different conclusions have been extracted regarding the potential of the different types of quality features considered for vulnerability detection and the best way to combine them.

Vulnerability detection solutions such as the one presented in this work may become of great importance in the biometric field as they can help to reduce the effect of direct attacks (those carried out at the sensor level and in consequence very difficult to detect), thus enhancing the level of security offered to those users that are more exposed to this type of threat.

ACKNOWLEDGMENT

This work has been partially supported by projects Tabula Rasa (FP7-ICT-257289) from EU, Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186) from Spanish MICINN, *Cátedra UAM-Telefónica*, and by the *Centro Criptológico Nacional*.

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, no. 2, pp. 125–143, 2006.

[2] A. Mansfield and J. Wayman, "Best practices in testing and reporting performance of biometric devices," CESG Biometrics Working Group, Tech. Rep., August 2002, (http://www.cesg.gov.uk/).

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication sytems," *IBM Systems Journal*, vol. 40, pp. 614–634, 2001.

[4] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio, "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," *Pattern Recognition Letters*, vol. 31, pp. 725–732, 2010.

[5] L. Thalheim and J. Krissler, "Body check: biometric access protection devices and their programs put to the test," *ct magazine*, pp. 114–121, November 2002.

[6] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics*, 2008.

[7] U. C. von Seelen, "Countermeasures against iris spoofing with contact lenses," Iridian Technologies, Tech. Rep., 2005.

[8] 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)*. Springer LNCS-5372, 2008, pp. 181–190.

[9] T. Van der Putte and J. Keuning, "Biometrical fingerprint recognition: don't get your fingers burned," in *Proc. Conference on Smart Card Research and Advanced Applications (CARDIS)*, 2000, pp. 289–303.

[10] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia, "An evaluation of indirect attacks and countermeasures in fingerprint verification systems," *Pattern Recognition Letters*, vol. 32, pp. 1643–1651, 2011.

[11] J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Bayesian hill-climbing attack and its application to signature verification," in *Proc. IAPR International Conference on Biometrics (ICB)*. Springer LNCS-4642, 2007, pp. 386–395.

[12] N. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proc. IAPR Audio- and Video-Based Person Authentication (AVBPA)*. Springer LNCS-2091, 2001, pp. 223–228.

[13] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," *Telecommunication Systems*, vol. 47, pp. 243–254, 2011.

[14] N. Poh, T. Bourlai, J. Kittler, L. Allano, F. Alonso-Fernandez, O. Ambekar, J. Baker, B. Dorizzi, O. Fatukasi, J. Fierrez, H. Ganster, J. Ortega-Garcia, D. Maurer, A. A. Salah, T. Sheidat, and C. Vielhauer, "Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms," *IEEE Trans. on Information Forensics and Security*, vol. 4, pp. 849–866, 2009.

[15] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun, "A comparative study of fingerprint image quality estimation methods," *IEEE Trans. on Information Forensics and Security*, vol. 2, no. 4, pp. 734–743, 2008.

[16] 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, Tech. Rep., 2003.

[17] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez, "BioSec baseline corpus: A multimodal biometric database," *Pattern Recognition*, vol. 40, pp. 1389–1392, 2007.

[18] Z. Wei, T. Tan, Z. Sun, and J. Cui, "Robust and fast assessment of iris image quality," in *Proc. IAPR Int. Conf. on Biometrics (ICB)*. Springer LNCS-3832, 2006, pp. 464–471.

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

[20] A. Abhyankar and S. Schukers, "Iris quality assessment and bi-orthogonal wavelet based encoding for recognition," *Pattern Recognition*, vol. 42, pp. 1878–1894, 2009.

[21] N. Kalka, J. Zou, N.Schmid, and B.Cubik, "Image quality assessment for iris biometric," in *Proc. SPIE Intl. Conf. on Biometric Technology for Human Identification III (BTHI III)*, vol. 6202, 2005, pp. 61 020D1–61 020D11.

[22] K. Bowyer, K. Hollingsworth, and P. Flynn, "Image understanding for iris biometrics: A survey," *Computer vision and Image Understanding*, vol. 110, pp. 281–307, 2007.

[23] J. Zou and N. A. Schmid, "Global and local quality measures for nir iris video," in *Proc. IEEE Workshops on Computer Vision and Pattern Recognition (WCVPR)*, 2009, pp. 120–125.

[24] L. Ma, T. Tan, Y. Wang, and D. Zhang, "Personal identification based on iris texture analysis," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 25, pp. 1519–1533, 2003.

[25] Y. Chen, S. C. Dass, and A. K. Jain, "Localized iris image quality using 2d wavelets," in *Proc. IAPR Int. Conf. on Biometrics (ICB)*, 2006, pp. 373–381.

[26] Y. Du, C. Belcher, Z. Zhou, and R.Ives, "Feature correlation evaluation approach for iris feature quality measure," *Signal Processing*, vol. 90, pp. 1176–1187, 2010.

[27] T. Matsumoto, "Artificial irises: importance of vulnerability analysis," in *Proc. Asian Biometrics Workshop (AWB)*, vol. 45, no. 8, 2004.

[28] M. Lane and L. Lordan, "Practical techniques for defeating biometric devices," Master's thesis, Dublin City Universtity, 2005.

[29] Z. Wei, X. Qiu, Z. Sun, and T. Tan, "Counterfeit iris detection based on texture analysis," in *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, 2008.

[30] A. Lefohn, B. Budge, P. Shirley, R. Caruso, and E. Reinhard, "An ocularist's approach to human iris synthesis," *IEEE Trans. on Computer Graphics and Applications*, vol. 23, pp. 70–75, 2003.

[31] P. Pudil, J. Novovicova, and J. Kittler, "Flotating search methods in feature selection," *Pattern Recognition Letters*, pp. 1119–1125, 1994.

[32] J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in *Proc. Intl. Joint Conf. on Biometrics (IJCB)*, 2011, submitted.

[33] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, J. Galbally, M. R. Freire, J. Gonzalez-Rodriguez, C. Garcia-Mateo, J.-L. Alba-Castro, E. Gonzalez-Agulla, E. Otero-Muras, S. Garcia-Salicetti, L. Allano, B. Ly-Van, B. Dorizzi, J. Kittler, T. Bourlai, N. Poh, F. Deravi, M. W. R. Ng, M. Fairhurst, J. Hennebert, A. Humm, M. Tistarelli, L. Brodo, J. Richiardi, A. Drygajlo, H. Ganster, F. M. Sukno, S.-K. Pavani, A. Frangi, L. Akarun, and A. Savran, "The multi-scenario multi-environment BioSecure multimodal database (BMDB)," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 32, pp. 1097–1111, 2010.

[34] ANSI-NIST, "ANSI x9.84-2001, biometric information management and security," 2001.

Iris Liveness Detection Based on Quality Related Features

Javier Galbally, Jaime Ortiz-Lopez, Julian Fierrez and Javier Ortega-Garcia
ATVS - Biometric Recognition Group, Universidad Autonoma de Madrid
C/ Francisco Tomas y Valiente 11, 28049 Madrid. SPAIN.
javier.galbally, jaime.ortiz, julian.fierrez, javier.ortega@uam.es

Abstract

A new liveness detection scheme for iris based on quality related measures is presented. The novel anti-spoofing technique is tested on a database comprising over 1,600 real and fake (high quality printed images) iris samples proving to have a very high potential as an effective protection scheme against direct attacks. Furthermore, the liveness detection method presented has the added advantage over previously studied techniques of needing just one iris image (the same used for verification) to decide whether it comes from a real or fake eye.

1. Introduction

Over the last recent years important research efforts have been conducted to study the vulnerabilities of biometric systems to direct attacks to the sensor (also known as *spoofing attacks*) which are very difficult to detect as they are carried out in the analog domain using synthetic biometric traits such as high quality iris printed images or gummy fingers [21], so that the digital protection mechanisms (digital signature, watermarking, etc.) are not valid to prevent them. Furthermore, the interest for the analysis of security vulnerabilities has surpassed the scientific field and different standardization initiatives at international level have emerged in order to deal with the problem of security evaluation in biometric systems, such as the Common Criteria through different Supporting Documents [5], or the Biometric Evaluation Methodology [3].

Among the different existing biometric traits, iris has been traditionally regarded as one of the most reliable and accurate. This fact has led researchers to pay special attention to its vulnerabilities and in particular to analyze to what extent their security level may be compromised by spoofing attacks [21, 26]. These attacking methods consist on presenting a synthetically generated iris to the sensor so that it is recognized as the legitimate user and access is granted. The most common and simple approaches are those carried out with high quality iris printed images [21, 25]. Finding an effective countermeasure against this type of attacking scheme is the problem addressed in the present paper. However, other more sophisticated threats have also been reported in the literature such as the use of contact lenses [26, 27] or even highly complex multilayered 3D artificial irises [17].

These research efforts in the study of the vulnerabilities of automatic recognition systems to direct attacks have clearly proven the necessity to propose and develop specific countermeasures against this type of security breach. In particular, different liveness detection methods have been presented through the past recent years. These algorithms are anti-spoofing techniques which use different physiological properties to distinguish between real and fake traits, thus improving the robustness of the system against direct attacks and increasing the security level offered to the final user. Iris liveness detection approaches can broadly be divided into:

- Software-based techniques. In this case fake irises are detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake eyes are extracted from the iris image, and not from the eye itself). These approaches include the detection of the four Purkinje reflections caused by each of the four optical surfaces comprised inside the eye [16], the detection of printed lenses through the texture analysis of the irises images [27], or the analysis of the brightness of the iris pattern [15].

- Hardware-based techniques. In this case some specific device is added to the sensor in order to detect particular properties of a living iris such as the eye hippus (which is the permanent oscillation that the eye pupil presents even under uniform lighting conditions) or the pupil response to a sudden lighting event (e.g., switching on a diode) [8], or measuring the infrared light reflections from the moist cornea [22].

Although hardware-based approaches usually present a higher detection rate, the software-based techniques have

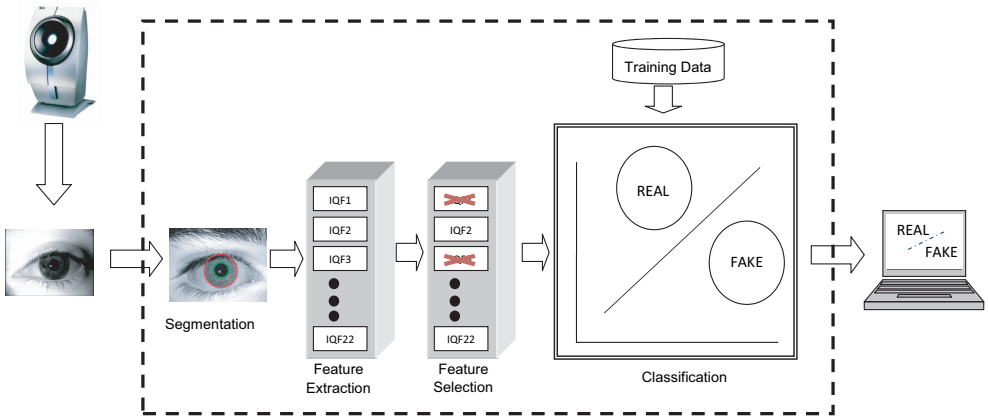


Figure 1. General diagram of the liveness detection system presented in this work.

the advantage of being less expensive (as no extra device in needed), and less intrusive for the user (very important characteristic for a practical liveness detection solution). In general, a combination of both type of anti-spoofing schemes would be the most desirable approach to increase the security level of biometric systems.

In the present work, we analyze the potential of quality assessment (already considered in the literature for multimodal fusion [23], or score rejection [2]) to identify real and fake iris samples acquired from a high quality printed image. It is not the first time quality assessment has been explored as a way to detect spoofing attacks. A similar strategy to the one proposed in the present paper based on quality related features has already been used for spoofing detection in fingerprint based recognition systems [11], achieving remarkable good results in the first International Fingerprint Liveness Detection Competition (LivDet 2009) [20]. Furthermore, some quality based features have also been used individually for liveness detection in traits such as iris [15, 27] or face [18].

We propose a new parameterization based on quality related measures which is used in a global software-based solution for iris liveness detection. This novel strategy has the clear advantage over other previously proposed methods of needing just one iris image (i.e., the same iris image used for access) to extract the necessary features in order to determine if the eye presented to the sensor is real or fake. This fact shortens the acquisition process and reduces the inconvenience for the final user. The presented method is tested on an iris database which comprises 1,600 real and fake (high quality printed images) samples where it has proven its high potential as a countermeasure to prevent spoofing attacks. Different conclusions are also extracted regarding the most convenient types of quality features to be considered in liveness detection.

The rest of the paper is structured as follows. The liveness detection system is described in Sect. 2, with special attention to the different features used. In Sect. 3 the database and protocol used in the experiments is presented, and results are given in Sect. 4. Conclusions are finally drawn in Sect. 5.

2. Liveness Detection System

The problem of liveness detection can be seen as a two-class classification problem where an input iris image has to be assigned to one of two classes: real or fake. The key point of the process is to find a set of discriminant features which permits to build an appropriate classifier which gives the probability of the image vitality given the extracted set of features. In the present work we propose a novel parameterization using quality related measures which is tested on a complete liveness detection system.

A general diagram of the liveness detection system presented in this work is shown in Fig. 1. Just one input is given to the system: the iris image to be classified (the same one used for verification). In the first step the iris is segmented from the background, for this purpose, a circular Hough transform is used in order to detect the iris and pupil boundaries as proposed in [25]. Once the useful information of the total image has been separated, twenty-two different quality measures are extracted which will serve as the feature vector that will be used in the classification. Prior to the classification step, the best performing features are selected using the Sequential Floating Feature Selection (SFFS) algorithm [24]. Once the final feature vector has been generated the iris is classified as real (generated by a living eye), or fake (coming from a synthetic trait).

2.1. Feature Extraction

The parameterization proposed in the present work and applied to liveness detection comprises twenty-two quality-based features adapted from different parameters described in the literature. From a biometric point of view, the qua-

Class	Features
Focus	*IQF1*, *IQF4*, *IQF15*, *IQF16*
Motion	*IQF2*, *IQF5*, *IQF18*, *IQF20*
Occlusion	*IQF3*, *IQF6-12*, *IQF17*, *IQF19*, *IQF21*
Others	*IQF13*, *IQF14*, *IQF22*

Table 1. Summary of the 22 quality related features implemented in this paper classified according to the iris characteristic measured.

lity of iris images can be assessed by measuring one of the following properties: i) focus, ii) motion blur, iii) occlusion, and iv) others including the contrast or the dilation of the pupil. A number of sources of information are used to measure these properties such as the high frequency power spectrum, angle information provided by directional filters, pixel intensity of certain eye regions, or different ratios comparing the iris area to that of the image, or the iris and pupil sizes. Iris quality can be assessed either analyzing the image in a holistic manner, or combining the quality from local blocks of the image.

In the following, we give some details about the quality measures implemented in this paper, together with a short explanation of the rationale behind the use of those parameters in the proposed anti-spoofing system and why they may be useful, *a priori*, for a liveness detection problem such as the one addressed in the present work. A summary of the different quality features used in this work and the characteristic that they measure (i.e., class to which they may be assigned) is given in Table 1.

2.1.1 Focus features

Iris printed images are a 2D surface in opposition to the 3D volume of a real eye for which acquisition devices are thought. Thus, it is expected that the focus of a fake iris will differ from that of a genuine sample.

Intuitively, an image with good focus is a sharp image. Thus, defocus primarily attenuates high spatial frequencies, which means that almost all features estimating this property perform some measure of the high frequency content in the overall image or in the segmented iris region. The different focus estimators considered in this work are given below. In Fig. 2 an example of the computation of these features for a real and fake iris is shown.

- **High Frequency Power 1 (*IQF4*)** [7], which measures the energy concentration in the high frequency components of the spectrum using a high pass convolution kernel of 8×8.
- **High Frequency Power 2 (*IQF1*)** [28], very similar to the previous *IQF4* but uses a modified version of size 5×5 of the high pass filter proposed in [7].

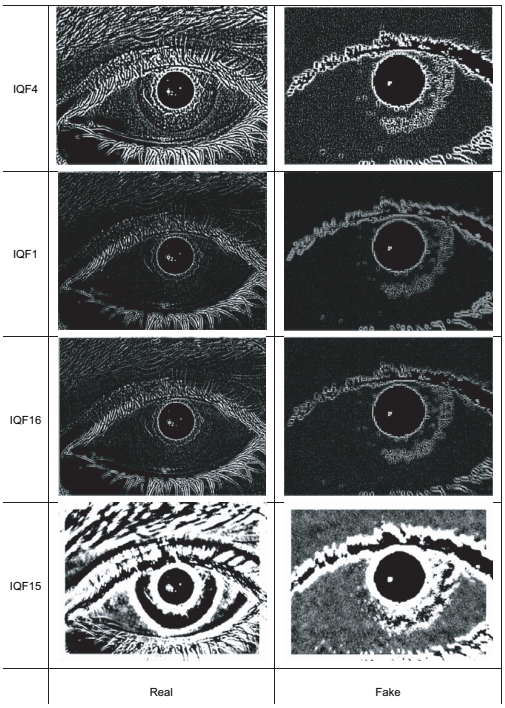


Figure 2. Example of the computation of the different focus quality features for a real and fake iris.

Figure 3. Power spectrum of a real and a fake iris images on its primary direction according to *IQF5*.

- **High Frequency Power 3 (*IQF16*)** [28], analog to the previous *IQF1* but a new high-pass 5×5 convolution kernel is proposed.
- **High Frequency Power 4 (*IQF15*)** [1], it estimates the defocus of the image by computing the second order derivative (using a discrete approximation of the modified Laplacian) in order to high pass the iris images.

2.1.2 Motion features

It is expected that the degree of movement of an iris printed on a sheet of paper and held in front of a sensor will be different from that of a real eye where a more steady position can be maintained so that the small trembling usually observed in the first case should be almost imperceptible.

Motion-related features try to estimate the image blur

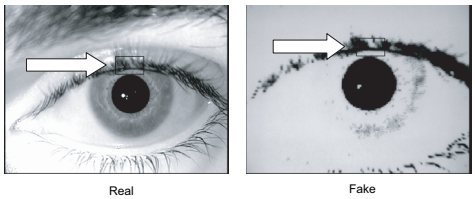


Figure 4. Region of interest used to estimate the iris occlusion according to *IQF3*.

caused by motion (of the iris or of the sensor). The effect of motion is generally reflected on the directionality of the image, thus, these estimators are usually based on the computation of the preponderant directions within a given iris sample.

- **Vertical High Frequency Power 1 (*IQF2*)** [28], it uses a variation of the Sum Modulus Difference (SMD) filter proposed by Jarvis in [13] in order to measure the vertical high frequency power as indicator of the motion blur degree.
- **Vertical High Frequency Power 2 (*IQF18*)** [4], analog to the previous *IQF2* but using a new version of the vertical SMD filter.
- **Directional Strength (*IQF5*)** [14], it searches for the primary direction of movement in the iris images using directional masks (five degrees rotation between them) and computing the total power of the resulting filtered images. Then the final quality measure is taken as the strength of the Fourier coefficients which fall within a narrow window perpendicular to the previously estimated primary direction. In Fig. 3 we show the primary direction computation for a real and a fake iris.
- **Global Spectral Information (*IQF20*)** [29], it estimates the motion and defocus blurs simultaneously by considering the global spectral information and the image/iris ratio (see *IQF19*) of the segmented iris image.

2.1.3 Occlusion features

Fake iris samples captured from a printed image usually present a different illumination than real images, appearing in the former very bright or dark sections which may be treated, in practice, as occluded areas. This can result in a different level of occlusion between real and fake samples that may lead to fake detection.

Occlusion-related features try to detect those areas of the iris which are occluded by some external element such as the eyelids or the eyelashes. In this case different heterogeneous schemes have been proposed in the literature studying in general local characteristics of the iris image.

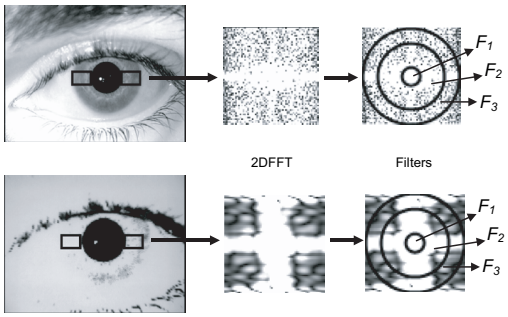


Figure 5. General process followed to estimate F_1, F_2 and F_3 for a real (top) and fake (bottom) iris. These parameters are then used for the computation of features *IQF6-12*.

- **Region of Interest (*IQF3*)** [28], it analyzes the average value of the pixels in the region of interest, located 50 pixels above the pupil center and shown in Fig. 4.
- **Frequency Distribution Rates 1 (*IQF6-12*)** [19], these are different combinations (adding, substracting, multiplying or dividing) of three different parameters which consider respectively the power of the low (F_1), medium (F_2), and high (F_3) frequencies (computed according to the 2D Fourier Spectrum) of two local regions in iris images. The process followed to compute these three parameters is depicted in Fig. 5. Although here are included in the occlusion class, these quality descriptors may also be used to estimate other quality characteristics such as the motion or defocus blur.
- **Frequency Distribution Rates 2 (*IQF17*)** [6], similar to the previous quality features *IQF6-12* but in this case the iris is divided into multiple frequency regions (not just low, medium and high) and the spectrum is computed according to the 2D Continuous Wavelet Transform (2DCWT) which is more suited for deriving local quality measures.
- **Iris/Image Ratio (*IQF19*)** [29], it computes the ratio between the area of the segmented iris and the whole image. Depending on the sensor used for the acquisition, the distance from the trait to the device in order to capture a valid image can be different for a 2D surface (fake iris) than for a 3D volume (real iris). This may lead to significant differences between the two types of samples that can be useful in liveness detection.
- **Binarization (*IQF21*)** [9], it estimates the iris area not occluded by eyelids, eyelashes and other elements by doing a binarization of the eye image.

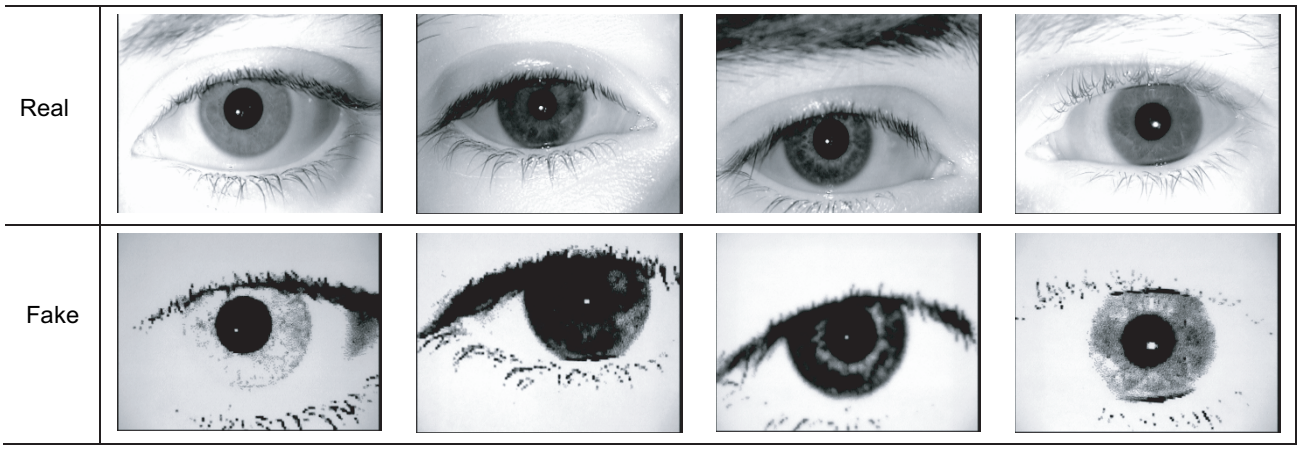


Figure 7. Typical real iris images and their corresponding fake samples that may be found in the database used in the experiments.

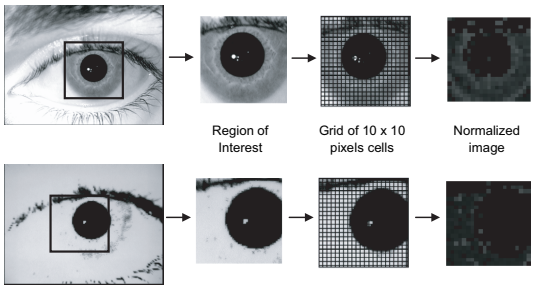


Figure 6. General process followed to compute *IQF13* for a real (top) and fake (bottom) iris image.

2.1.4 Other features

In this category are included all those features measuring some different iris characteristic to those considered in the previous classes and which may be *a priori* useful for liveness detection. In particular, the two quality indicators taken into account here will be the contrast (similar to occlusion) and the pupil dilation:

- **Global Contrast (*IQF14*)** [1]. This parameter detects extremely bright or dark parts of the image (more common in fake iris samples). For images with 256 grey levels, pixels with very high or low values are set to a contrast value of 0 while the rest are normalized to a scale of 1-25.

- **Local Contrast (*IQF13*)**, this novel quality feature proposed in the present work is inspired in the technique presented in [1] for occlusion estimation. A square region covering the iris and pupil is divided into a 10×10 cell grid. Each cell is assigned a value which corresponds to the power of its medium frequencies. The final quality measure is obtained averaging the number of cells which value falls between 20 and 60 by the total number of cells. The general process to compute *IQF13* is depicted in Fig. 6.

- **Pupil Dilation (*IQF22*)** [9], it computes the ratio between the pupil and iris radios.

2.2. Feature Selection and Classifier

Due to the curse of dimensionality, it is possible that the best classifying results are not obtained using the set of twenty-two proposed features, but a subset of them. As we are dealing with a twenty-two dimensional problem there are $2^{22}-1$ possible feature subsets, which makes unfeasible to perform exhaustive search. For this reason Pudil's Sequential Floating Feature Selection (SFFS) algorithm [24] is used as feature selection method as it has proven before a very good performance compared to other feature selection techniques [12].

For classification we have used a standard quadratic classifier fitting the training data with multivariate normal densities with diagonal covariance estimates stratified by group.

3. Database

The database used in the experiments comprises real and fake iris images of 50 users of the BioSec baseline database [10]. This fake iris database was acquired in the frame of a research work to evaluate the vulnerabilities of iris verification systems to direct attacks [25]. In that work, the spoofing attacks carried out on these data achieved a success rate of over 30% for all the different scenarios tested. The high performance of the direct attacks described in [25] proves that the fake samples considered in the present work pose a real threat to iris-based biometric systems.

The fake samples were acquired following a three step process which is further detailed in [25]: i) first original images were processed to improve the final quality of the fake irises, ii) then they were printed using a high-quality

# features	Feature Subset	Class	ACE_{train} (%)	ACE_{test} (%)
1	*IQF6*	Occlusion	19.25	24.00
	IQF10	Occlusion	19.25	20.87
	IQF11	Occlusion	18.50	22.50
	IQF13	Contrast	5.75	7.37
	IQF19	Occlusion	4.25	10.5
	IQF21	Occlusion	14.75	14.62
2	*IQF19* + *IQF4*	Occlusion + focus	2.25	5.00
	IQF19 + *IQF13*	Occlusion + contrast	0.25	3.00
	IQF19 + *IQF14*	Occlusion + contrast	2.75	6.50
	IQF19 + *IQF15*	Occlusion + focus	2.50	4.75
	IQF19 + *IQF21*	Occlusion + occlusion	4.00	5.37
	IQF19 + *IQF22*	Occlusion + dilation	0.00	0.00
3	*IQF19* + *IQF22* + *IQF13*	Occ. + dilat. + contrast	0.00	0.00
+ 3	*IQF19* + *IQF22* + *IQF13* + any	Occ. + dilat. + contrast + any	0.00	0.00

Table 2. Classification results for the best feature subsets. ACE_{train} and ACE_{test} represent respectively the Average Classification Error in the train and test sets.

commercial printer, and last iii) the printed images were presented to the iris sensor in order to obtain the fake image.

The database follows the same structure as the original BioSec database, therefore, the data used in the experiments comprises 50 users $\times$ 2 eyes $\times$ 4 images $\times$ 2 sessions $=$ 800 fake iris images and its corresponding original samples. The acquisition of both real and fake samples was carried out using the LG IrisAccess EOU3000 sensor. In Fig. 7 we show some typical real and fake iris images that may be found in the dataset.

For the experiments the database is divided into a train set (comprising 200 real images and their corresponding fake samples) where the feature selection process and the classifier training are performed, and a totally independent test set (with the remaining 600 real and fake samples) to evaluate the performance of the proposed liveness detection approach.

4. Results

The first objective of the experiments is to find the optimal feature subsets (out of the proposed 22 feature set) for the considered database using the SFFS feature selection algorithm. The fitness function to be optimized by the algorithm for each of the subsets is the classification performance computed on the train set in terms of the Average Classification Error, which is defined as ACE $=$ (FLR $+$ FFR)$/2$, where the FLR (False Living Rate) represents the percentage of fake fingerprints misclassified as real, and the FFR (False Fake Rate) computes the percentage of real fingerprints assigned to the fake class.

Once the optimal subsets have been found and evaluated using the train set, their performance is finally assessed on the test set (which has no overlap with the training samples) in order to obtain totally unbiased results about the discriminant capabilities of the system. In Table 2 we summarize the results obtained in the classification process. For clarity, only the best feature subsets in the training phase are given. The performance results shown correspond to the classification threshold where FLR=FFR=ACE.

Several observations may be extracted from the results shown in Table 2: i) the proposed system presents a very high potential as a new method to prevent direct attacks, reaching a 100% of correctly classified samples for the particular fake data considered; ii) for the fake samples taken into account (high quality iris printed images) and for the sensor used, the occlusion features seem to present the best single performance for liveness detection; iii) when several features are combined the best performance is reached for complementary parameters measuring each of them a different characteristic from the iris image (e.g., see the best combination for 3 or more features).

As was explained in the description of the occlusion parameters (see Sect. 1), some of these features measure the difference in illumination that exists between real 3D irises (uniform illumination) and fake 2D samples (very bright or dark areas). This fact can account for the very good individual behaviour presented by this type of quality measures in the liveness detection problem addressed.

5. Conclusions

A novel liveness detection scheme for iris, based on quality related measures has been presented. The proposed method was tested on an iris database which comprises 1,600 real and fake images, where it reached a total 100% of correctly classified (real or fake) samples, proving this way its high potential as a countermeasure to prevent direct attacks to the sensor. Furthermore, different conclusions have been extracted regarding the potential of the different types of

quality features considered for liveness detection and the best way to combine them.

Although the results presented in this work have been obtained for a specific type of synthetic traits (i.e., high quality iris printed images), we firmly believe that the proposed method can also be used to detect other types of fake data (e.g., printed lenses) by selecting the subset of parameters that better adapts to the new anti-spoofing problem. Even though the very high performance shown for the tested database may not be generalized, we do think these results give an idea of the high potential of the proposed method. In fact, it should not be an easy task to generate such a synthetic trait that it possesses all the measured quality related features in the same degree as a real sample.

Liveness detection solutions such as the one presented in this work are of great importance in the biometric field as they help to prevent direct attacks (those carried out with synthetic traits, and very difficult to detect), enhancing this way the level of security offered to the user.

6. Acknowledgements

This work has been partially supported by projects Contexts (S2009/TIC-1485) from CAM, Bio-Challenge (TEC2009-11186) from Spanish MICINN, TABULA RASA (FP7-ICT-257289) from EU, and Catedra UAM- Telefonica.

References

[1] A. Abhyankar and S. Schukers. Iris quality assessment and bi-orthogonal wavelet based encoding for recognition. *Pattern Recognition*, 42:1878–1894, 2009. 3, 5

[2] F. Alonso-Fernandez, J. Fierrez, J. Ortega-Garcia, J. Gonzalez-Rodriguez, H. Fronthaler, K. Kollreider, and J. Bigun. A comparative study of fingerprint image quality estimation methods. *IEEE Trans. on Information Forensics and Security*, 2(4):734–743, 2008. 2

[3] BEM. Biometric Evaluation Methodology. v1.0, 2002. 1

[4] K. Bowyer, K. Hollingsworth, and P. Flynn. Image understanding for iris biometrics: A survey. *Computer vision and Image Understanding*, 110:281–307, 2007. 4

[5] CC. Common Criteria for Information Technology Security Evaluation. v3.1, 2006. Available on-line at http://www.commoncriteriaportal.org/. 1

[6] Y. Chen, S. C. Dass, and A. K. Jain. Localized iris image quality using 2d wavelets. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 373–381, 2006. 4

[7] J. Daugman. How iris recognition works. *IEEE Trans. on Circuits and Systems for Video Technology*, 14:21–30, 2004. 3

[8] J. Daugman. Iris recognition and anti-spoofing countermeasures. In *Proc. Int. Biometrics Conf. (IBC)*, 2004. 1

[9] Y. Du, C. Belcher, Z. Zhou, and R.Ives. Feature correlation evaluation approach for iris feature quality measure. *Signal Processing*, 90:1176–1187, 2010. 4, 5

[10] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez. BioSec baseline corpus: A multimodal biometric database. *Pattern Recognition*, 40:1389–1392, 2007. 5

[11] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia. A high performance fingerprint liveness detection method based on quality related features. *Future Generation Computer Systems*, 28:311–321, 2012. To appear. 2

[12] A. K. Jain and D. Zongker. Feature selection: evaluation, application, and small sample performance. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 19:153–158, 1997. 5

[13] R. A. Jarvis. Focus optimization criteria for computer image processing. *Microscope*, 24:163–180, 1976. 4

[14] N. Kalka, J. Zou, N.Schmid, and B.Cubik. Image quality assessment for iris biometric. In *Proc. SPIE Intl. Conf. on Biometric Technology for Human Identification III (BTHI III)*, volume 6202, pages 61020D1–61020D11, 2005. 4

[15] M. Kanematsu, H. Takano, and K. Nakamura. Highly reliable liveness detection method for iris recognition. In *Proc. SICE Annual Conference, Int. Conf. on Instrumentation, Control and Information Technology (ICICIT)*, pages 361–364, 2007. 1, 2

[16] E. C. Lee, K. R. Park, and J. Kim. Fake iris detection by using purkinje image. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 397–403, 2006. 1

[17] A. Lefohn, B. Budge, P. Shirley, R. Caruso, and E. Reinhard. An ocularist's approach to human iris synthesis. *IEEE Trans. on Computer Graphics and Applications*, 23:70–75, 2003. 1

[18] J. Li, Y. Wang, T. Tan, and A. K. Jain. Live face detection based on the analysis of fourier spectra. In *Proc. SPIE Biometric Technology for Human Identification (BTHI)*, pages 296–303, 2004. 2

[19] L. Ma, T. Tan, Y. Wang, and D. Zhang. Personal identification based on iris texture analysis. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 25:1519–1533, 2003. 4

[20] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, A. Tidu, F. Roli, and S. Schuckers. First international fingerprint liveness detection competition – livdet 2009. In *Proc. IAPR Int. Conf. on Image Analysis and Processing (ICIAP)*, pages 12–23. LNCS-5716, 2009. 2

[21] T. Matsumoto. Artificial irises: importance of vulnerability analysis. In *Proc. Asian Biometrics Workshop (AWB)*, volume 45, 2004. 1

[22] A. Pacut and A. Czajka. Aliveness detection for iris biometrics. In *Proc. IEEE Int. Carnahan Conf. on Security Technology (ICCST)*, pages 122–129, 2006. 1

[23] N. Poh, T. Bourlai, J. Kittler, L. Allano, F. Alonso-Fernandez, O. Ambekar, J. Baker, B. Dorizzi, O. Fatukasi, J. Fierrez, H. Ganster, J. Ortega-Garcia, D. Maurer, A. A. Salah, T. Sheidat, and C. Vielhauer. Benchmarking quality-dependent and cost-sensitive score-level multimodal biometric fusion algorithms. *IEEE Trans. on Information Forensicsand Security*, 4:849–866, 2009. 2

[24] P. Pudil, J. Novovicova, and J. Kittler. Flotating search methods in feature selection. *Pattern Recognition Letters*, pages 1119–1125, 1994. 2, 5

[25] 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)*, pages 181–190. Springer LNCS-5372, 2008. 1, 2, 5

[26] U. C. von Seelen. Countermeasures against iris spoofing with contact lenses. Technical report, Iridian Technologies, 2005. 1

[27] Z. Wei, X. Qiu, Z. Sun, and T. Tan. Counterfeit iris detection based on texture analysis. In *Proc. IAPR Int. Conf. on Pattern Recognition (ICPR)*, 2008. 1, 2

[28] Z. Wei, T. Tan, Z. Sun, and J. Cui. Robust and fast assessment of iris image quality. In *Proc. IAPR Int. Conf. on Biometrics (ICB)*, pages 464–471. Springer LNCS-3832, 2006. 3, 4

[29] J. Zou and N. A. Schmid. Global and local quality measures for nir iris video. In *Proc. IEEE Workshops on Computer Vision and Pattern Recognition (WCVPR)*, pages 120–125, 2009. 4