

# Reconocimiento biométrico de iris en ambientes de alta seguridad

Juan Alberto Devincenzi<sup>1</sup>, María Laura Finamore<sup>1</sup>, Franco Chichizola<sup>2</sup>, Laura De Giusti<sup>2</sup>, Marcelo Naiouf<sup>2</sup>

<sup>1</sup>Facultad de Informática, Universidad Nacional de La Plata,  
La Plata, Argentina  
{jdevlaplata, lfinamore}@gmail.com

<sup>2</sup>Instituto de Investigación en Informática LIDI - Facultad de Informática, UNLP  
La Plata, Argentina  
{francoch, ldogiusti, mnaiouf}@lidi.info.unlp.edu.ar

**Abstract.** En este trabajo se presenta el uso de identificación biométrica por medio del reconocimiento de iris, en ambientes específicos que requieran alto nivel de seguridad, como por ejemplo las penitenciarías. Se analizan diferentes algoritmos existentes tales como Extraction of Complex Wavelet Features for Iris Recognition (CWF), DCT-Based Iris Recognition (DCT) e Iris recognition Based on Multichannel Gabor Filtering (MGF), con el objetivo de compararlos y determinar su adaptabilidad a estos entornos. La elección de estos tres algoritmos se debe a los buenos resultados presentados por ellos tanto en la identificación como en la verificación de identidad.

A partir de las características más relevantes de los algoritmos analizados se presenta el desarrollo de un sistema de identificación para utilizar en el ámbito antes mencionado. Para determinar el comportamiento del sistema se comparan los resultados obtenidos con los analizados previamente.

Los resultados logrados permiten indicar que la implementación propuesta tiene un muy buen funcionamiento al trabajar con imágenes que poseen las mismas características que las que se pueden obtener en el ambiente requerido.

**Palabras Claves:** Reconocimiento Biométrico, Seguridad, Identificación, Procesamiento de imágenes, Extracción de características.

## 1 Introducción

Vivimos en una sociedad en donde el hombre, por cuestiones relacionadas con la seguridad, se ve ante la necesidad de controlar el acceso a determinados lugares o información, e incluso a identificarse unívocamente entre otros.

En el ámbito de seguridad carcelaria en particular, el reconocimiento unívoco de la persona es de mayor importancia debido a que un fallo genera una serie de consecuencias que pueden ser drásticas, tanto para la institución, como para la población. Por ejemplo: desconocer la peligrosidad de un recluso, otorgar o denegar la libertad a una persona errónea, repetir información para una misma persona, entre otras.

Basándose en estudios recogidos en [1], en el patrón visual del iris hay más información que identifica unívocamente a una persona que en una huella dactilar. De hecho, los dos ojos de una persona poseen patrones distintos, siendo esta una característica muy importante que debe ser considerada en el sistema, al no ser la imagen de los dos ojos intercambiables. A partir de esto se puede concluir que la técnica presenta una unicidad extremadamente alta, lo cual incrementa su viabilidad para ser utilizada en identificación en entornos de alta seguridad.

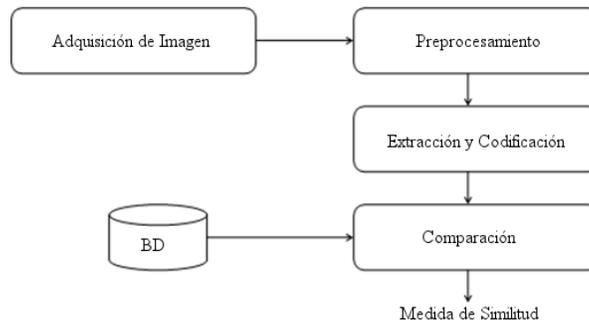
Teniendo en cuenta las condiciones de un ámbito carcelario, el reconocimiento de iris resulta ser apropiado para la identificación de las personas privadas de su libertad. Los motivos de esto son:

- No existe la necesidad de contacto físico entre el dispositivo y la persona a identificar.
- Es muy difícil y peligroso alterar el iris en forma voluntaria (esto no ocurre con las huellas y el rostro), lo cual otorga un alto grado de seguridad.
- El resultado del proceso de identificación de un individuo se puede realizar en tiempo real.
- Los resultados de identificación presentan mejor desempeño respecto de otros métodos biométricos.

En el resto de las secciones se detalla brevemente el funcionamiento general de un sistema biométrico de iris, luego se describen de manera concisa los algoritmos analizados y se especifica la base de imágenes utilizada [2] y las razones de su elección, para luego poder realizar las pruebas sobre los algoritmos seleccionados y en la siguiente sección se muestra una comparación de los resultados de las implementaciones. En la sección 4 se describe el algoritmo implementado para este trabajo y se presentan los resultados obtenidos comparándolo con aquel algoritmo que mejor resultado presentó; por último, se presentan las conclusiones finales.

## 2 Sistema biométrico de iris

En un sistema de identificación biométrica se debe realizar una serie de pasos generales (no siempre se deben hacer todos ellos) como muestra la Fig. 1.



**Fig. 1.** Etapas generales de un sistema de identificación biométrica de iris.

En el caso particular de los sistemas de identificación por medio del iris, en cada una de estas etapas se debe realizar un subconjunto de acciones, las cuales se detallan a continuación:

- *Adquisición*: es la obtención de la imagen del iris con un dispositivo determinado.
- *Preprocesamiento*: esta etapa se divide en la etapa de segmentación, normalización y mejora.
  - En la etapa de *segmentación* se aísla al iris del resto de la imagen. Si el iris no es aislado correctamente puede dificultarse la correcta identificación.
  - En la etapa de *normalización* se logra que la imagen del iris aislada sea independiente del tamaño de la pupila, debido a que puede variar en cada imagen. Normalizar la imagen implica transformar la región anular del iris en una región rectangular de dimensiones constantes
  - La etapa de *mejora* prepara a la imagen normalizada modificándola y preparándola para la etapa de extracción.
- *Extracción y codificación*: en este punto se obtiene la representación de cada imagen (o iris) para poder ser comparada fácilmente con el resto de las imágenes.
  - En la etapa de *extracción* distintos métodos pueden ser utilizados para extraer las características de una imagen, entre los que se pueden mencionar 2D-CWT, DCT, Filtro de Gabor, entre otros.
  - En la etapa de *codificación*, se genera una plantilla o vector de características codificadas mediante algún método seleccionado, que permitirá reconocer a la persona.
- *Comparación*: en esta etapa se computa una medida de diferencia entre las plantillas comparadas, y en base a esta medida se decide si los códigos han sido generados por el mismo iris o no. Entre los métodos más utilizados pueden mencionarse la Distancia Hamming y la Distancia Euclidiana para realizar la verificación (determinar si la persona es quien dice ser) o la identificación (determinar la identidad de un individuo, comparando la imagen contra toda la Base de Datos).

### 3 Análisis de algoritmos existentes

Teniendo en cuenta diferentes algoritmos existentes para identificación biométrica por medio del Iris, se analizan detalladamente tres de ellos: Extraction of Complex Wavelet Features for Iris Recognition (CWF) [3], DCT-Based Iris Recognition (DCT) [4] e Iris recognition Based on Multichannel Gabor Filtering (MGF) [5]. La elección de estos algoritmos se debe a que se adaptan a las características del entorno donde se deben usar, obteniendo buenos resultados en cuanto a la verificación e identificación.

En la Tabla 1 se resumen las características de cada uno de ellos en las diferentes etapas descriptas en la sección 2.

**Tabla 1.** Características de los algoritmos analizados

<b>Etapa</b>	<b>CWF</b>	<b>DCT</b>	<b>MGF</b>
<i>Preprocesamiento</i>	Transformada de Hough. Ecuilización de histograma.	Borde del iris buscando cambios bruscos de nivel de gris. Eliminación de iluminación de fondo. Funciones ventana. Filtro gaussiano.	
<i>Extracción</i>	Transformada de Wavelet Continua.	Transformada de Coseno Discreta.	Filtro de Gabor.
<i>Codificación</i>	Demodulación de fase cuadrante.	Obtención de los cruces en 0 de las diferencias de los parches adyacentes.	Aplicación de filtro de Gabor. Aplicación del promedio de desviación absoluta.
<i>Comparación</i>	Distancia de hamming.	Distancia de hamming.	Distancia euclidiana con pesos.

### 3.1 Base de datos utilizada

Existe una gran cantidad de bases de imágenes de iris que permiten determinar la eficacia de los algoritmos. Una de estas es la base Syn [2], que es la utilizada en este trabajo.

Posee una gran cantidad de imágenes (1.000 personas, cada una con 10 imágenes) con características particulares, entre las que se pueden mencionar: deformación, borrosidad, rotación, puntos luminosos y en formato JPG, lo que implica una pérdida de calidad. Estas características permiten simular intentos de fraude, como se espera que suceda en el ámbito que se desea utilizar.

Las características mencionadas anteriormente de las imágenes de la base permiten simular el ambiente donde se debe utilizar el sistema, por lo que presenta un desafío para los algoritmos que permite verificar la adaptación a este tipo de escenario.

Otras de las características a destacar de las imágenes de la base seleccionada, son: el tamaño en disco promedio de cada imagen es de 20 Kbytes, y el tamaño en disco de la base de imágenes en su totalidad es de 192 Mbytes, lo que la hace una base de imágenes económica de mantener.

Otra ventaja en el uso de la base de imágenes Syn es que el dispositivo que se utiliza para la captura es de fabricación casera, a diferencia de otras bases de imágenes cuyo dispositivo de captura es de un costo superior.

### 3.2 Pruebas realizadas con algoritmos existentes

Se realizó una serie de pruebas con los tres algoritmos seleccionados, utilizando la base de imágenes mencionada en el apartado 3.1 para un total de 100 personas distintas, con 3 imágenes para la etapa de enrolamiento y 4 para la etapa de identificación.

En la Tabla 2 se muestran los resultados de las pruebas, indicando:

- *Porcentaje de aciertos en la identificación*: es el porcentaje de personas identificadas correctamente sobre la totalidad de las personas que conformaron la prueba.
- *Porcentaje de aciertos en la verificación (Aceptación/Rechazo)*: es el porcentaje de personas correctamente verificadas sobre la totalidad de personas que conforman la prueba.

**Tabla 2.** Resultados obtenidos con los algoritmos existentes.

	<b>CWF</b>	<b>DCT</b>	<b>MGF</b>
Porcentaje de aciertos en la identificación	83%	81%	68%
Porcentaje de aciertos en la verificación (aceptación)	85%	61%	61%
Porcentaje de aciertos en la verificación (rechazo)	82%	100%	94%

A partir de los resultados obtenidos, CWF resulta ser el más conveniente, debido a que arroja mejores resultados en general, y responde de manera más adecuada a las necesidades de ambientes de alta seguridad como las penitenciarías.

## 4 Descripción del Sistema de identificación desarrollado

Basado en los tres algoritmos indicados en la sección 3 (CWF, DCT y MGF), y después de analizar los problemas de estos (o mejoras a realizar), se desarrolla un nuevo algoritmo para utilizar en el sistema de identificación biométrica orientado a ambientes de alta seguridad. A continuación se detalla dicho algoritmo para cada una de las etapas mencionadas en la sección 2.

### 4.1 Adquisición

En esta etapa para obtener las imágenes, es necesario tener en cuenta que la iluminación debe estar dispuesta circularmente alrededor del sensor para asegurarse

de que el iris es iluminado de manera uniforme. Además cabe mencionar que sólo se utilizó un dispositivo de fabricación casera para la obtención de las mismas.

## 4.2 Preprocesamiento

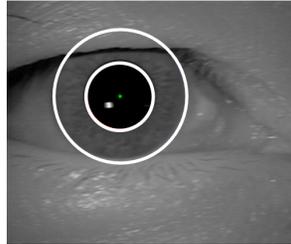
En esta etapa se procesa la imagen obtenida en 4.1, para obtener las características requeridas en la etapa 4.3. Como se menciona en la sección 2, se debe realizar la segmentación, normalización y mejora de la imagen.

### 4.2.1 Segmentación

Se obtienen los límites del iris, tanto interior, como exterior, considerándolos como círculos concéntricos. Para llevar a cabo la segmentación es necesario realizar las etapas que se describen a continuación:

1. *Reducción de la imagen*: para trabajar sólo con los objetos de interés. En este caso, la imagen resultante es de un tamaño de 420 x 500 píxeles.
2. *Eliminación de puntos luminosos*: debido a que los puntos luminosos de la imagen original deforman la imagen binarizada de la pupila, y esto dificulta detectarla correctamente, son removidos de la imagen erosionando los píxeles [6] que forman dichos objetos.
3. *Binarización - Erosión y Dilatación*: se realiza la binarización de la imagen conforme un determinado umbral. Luego se aplican las operaciones morfológicas de erosión y dilatación (con operadores de disco) para obtener la imagen donde se excluyan regiones que no necesitan ser procesadas.
4. *Detección del borde de la pupila*: se aplica el operador Sobel.
5. *Eliminación de objetos innecesarios*: se eliminan aquellos objetos de la imagen que pueden interferir en el momento de detectar el iris y la pupila. Se utiliza un método de eliminación de objetos conectados por 8 vecinos, cuya área sea menor a  $\pi \times r_p$ , siendo  $r_p$ , el radio de la pupila [3].
6. *Hallar coordenadas y radio de la pupila*:
  - *Encontrar blanco inferior*: en una primera instancia se detecta el punto inferior del borde de la pupila (este se localiza buscando el punto inferior de la imagen binarizada). A partir de allí, se buscan los puntos de corte con el borde hallado (a izquierda y derecha). Para hallar el punto blanco inferior, se busca entre las columnas 100 y 300 de la imagen (cuya resolución es de 420 x 500 píxeles) todos los puntos blancos. Esto se lleva a cabo de esta manera, pues ya se sabe que la pupila se encuentra entre estas columnas. Finalmente, de este conjunto, se obtiene el punto cuya fila sea la de mayor valor, es decir que se encuentre visualmente más abajo en la imagen.
  - *Encontrar el radio de la pupila*: a partir del punto blanco inferior hallado anteriormente, se buscan 10 puntos de corte (a izquierda y derecha) con el borde obtenido anteriormente, al aplicarse el operador Sobel. Posteriormente, se obtiene la máxima distancia entre estos logrando una mejor representación del radio de la pupila.

- *Encontrar el centro de la pupila:* una vez hallado el radio de la pupila, es necesario aplicar la transformada de Hough [6], para la detección del centro de la misma.
7. *Hallar el radio del iris:* para llevar esto a cabo, se utiliza la implementación propuesta por [4].



**Fig. 2.** Resultado de la obtención del radio de la pupila e iris.

#### 4.2.2 Normalización

*Realizar la transformación a coordenadas polares:* luego de obtener el centro y radio de la pupila y del iris (debido a que se los puede considerar concéntricos, aunque no necesariamente lo sean), la región anular obtenida es normalizada a una imagen rectangular, es decir que la imagen es “estirada”, recorriéndola en sentido antihorario para representarla en el eje polar, realizando las transformaciones correspondientes [3].

#### 4.2.3 Mejora

Se realizan mejoras sobre la imagen para obtener un mayor detalle de las características del iris. A continuación se describen las etapas realizadas:

- *Ecuilibración de histograma:* con la imagen normalizada se aplica la ecualización del histograma para generar una imagen con menor ruido, y resaltar sus características.
- *Eliminación de iluminación de fondo:* se mejora la imagen de manera que se vean resaltadas las características que hacen al patrón del iris. A la imagen normalizada se la dilata y erosiona con un operador de tipo disco, y esto se resta de la imagen normalizada. A este resultado se le ajusta la iluminación y se obtiene su histograma para luego ecualizar la imagen normalizada original con el histograma obtenido anteriormente [4].
- *Interpolación bilineal:* en la normalización, la imagen del iris que es angular, es estirada en un arreglo bidimensional. Debido a que no es mapeada exactamente como en la imagen original, se utiliza interpolación bilineal con los vecinos más próximos, la cual se logra promediando 4 píxeles adyacentes. De esta manera, se evita una mayor pérdida de información.
- *Redimensión de la imagen:* se redimensionan todas las plantillas normalizadas a un tamaño común, con el fin de que la extracción de características se realice sobre imágenes del mismo tamaño.

### 4.3 Extracción y codificación de características

En las siguientes etapas se extraen las características del iris normalizado y se codifican para ser utilizadas en la etapa de comparación.

#### 4.3.1 Extracción de características

La extracción de características se lleva a cabo en dos partes:

1. *FFT2*: se aplica la transformada de Fourier de dos dimensiones sobre la imagen normalizada, transformando la imagen del dominio del tiempo al dominio de la frecuencia y así lograr una mayor eficiencia en la obtención de resultados [6].
2. *2D-CWT*: luego de aplicar la transformada de Fourier, cada imagen normalizada se descompone utilizando el operador 2D-CWT, el cual permite descomponer la imagen en coeficientes reales e imaginarios, para luego codificarlos [3]. Para ejecutar este paso, se utilizó la *toolbox yawtb* [7] para el entorno de desarrollo Matlab, que proporciona este método entre los disponibles en la toolbox.

#### 4.3.2 Codificación de características

En esta etapa, el método utilizado se basa en la demodulación de fase cuadrante del vector de coeficientes. Consiste en tomar el valor real e imaginario de cada posición, y dependiendo del signo de cada uno, se codifica a binario [3] [8].

### 4.4 Comparación

En esta etapa se utiliza la *Distancia Hamming* para obtener la diferencia entre códigos obtenidos en la codificación de características para imágenes distintas. [3] [8].

La distancia entre dos códigos *A* y *B* se calcula mediante la Ecuación 1:

$$HD = \frac{\| \text{vectorA} \otimes \text{vectorB} \|}{\text{anchoDelVector} \times \text{altoDelVector}} \quad (1)$$

Donde, el símbolo  $\otimes$  es la operación lógica *XOR* y el operador  $\| \|$  computa la cantidad de bits iguales a uno. El numerador de la ecuación corresponde a la cantidad en que difieren los *códigos A* y *B*. Mediante la operación *XOR* se obtiene una matriz formada por valores uno, en las ubicaciones donde el *código A* y *B* son iguales y por cero donde difieren. En el denominador de la ecuación se computa la cantidad de bits comparados entre los códigos, de esta manera la distancia de Hamming obtenida es una medida porcentual de la diferencia entre los códigos comparados [3].

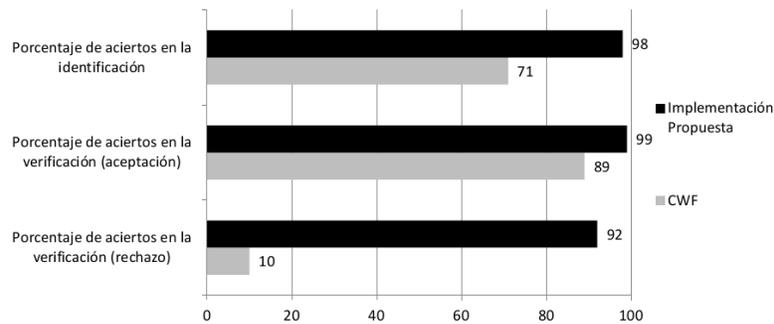
## 5 Resultados obtenidos

Para analizar el comportamiento del algoritmo presentado, se realizaron las pruebas del mismo usando la base de imágenes indicada en 3.1. En este caso se tuvieron en

cuenta las imágenes de las 1000 personas de la base, usando cinco para el enrolamiento y cinco para la identificación por persona.

Teniendo en cuenta los resultados de la sección 3.2, se puede ver que de los 3 algoritmos analizados el que mejores resultados obtiene es el CWF. Por esta razón, es el utilizado para comparar con el algoritmo propuesto.

En la Figura 3 se muestra la comparación de los resultados obtenidos utilizando las mismas métricas que de la sección 3.2: porcentaje de aciertos en la identificación, porcentaje de aciertos en la verificación (de aceptación), porcentaje de aciertos en la verificación (de rechazo).



**Fig. 3.** Comparación de los resultados obtenidos entre el algoritmo CWF y la implementación propuesta para 1000 personas.

Como resultado de la comparación se puede observar que el algoritmo propuesto se comporta mejor en todos los tipos de prueba. Entre las pruebas se puede destacar que para la identificación es un 27% más de aciertos que en CWF, mientras que para la verificación (por acierto) se llega a un 10% de mejora. Por otro lado, la diferencia más significativa se obtiene en las pruebas de verificación por rechazo (82%), aunque no es el uso más común para el algoritmo en este tipo de ambientes (penitenciarias).

Como principal resultado, se puede apreciar que la implementación propuesta logra un muy buen desempeño (cercano al 100% en los tres tipos de pruebas) como es necesario obtener en este tipo de ambientes, sobre todo en el momento de verificar que alguien es quien dice ser (o se piensa que es).

## 6 Conclusiones y líneas de trabajo futuro

En este trabajo se analizan, implementan y testean tres algoritmos existentes para identificación biométrica por medio del iris (CWF, DCT, MGF). De las pruebas realizadas se puede observar que CWF presenta los mejores resultados tanto para la identificación como para la verificación.

A partir de este análisis se implementó un algoritmo que combina varias características de los tres estudiados y se agregaron mejoras significativas para lograr un buen desempeño orientando su desarrollo para que sea utilizado en ambientes de alta seguridad como las penitenciarías.

Para determinar su comportamiento en estos entornos, se realizaron pruebas utilizando imágenes con características similares a las que se podrían encontrar en este tipo de ámbitos (base de imágenes Syn). Los resultados experimentales muestran que el nuevo algoritmo presentado, logra un muy buen desempeño para este tipo de entornos de seguridad, en ambas situaciones (identificación y verificación).

Al comparar estos resultados con los obtenidos por el algoritmo CWF (el mejor de los tres analizados) se puede ver que, en la identificación se obtienen mejoras superiores al 25%, y en la etapa de verificación, en la aceptación supera al algoritmo CWF en un 10% y en el rechazo logra superarlo en un 80%.

Otro punto a tener en cuenta, es que el dispositivo que se utiliza para la captura de las imágenes requeridas en el sistema desarrollado es de fabricación casera, con la ventaja económica y de asequibilidad que le corresponde.

Considerando las propiedades de esas imágenes, y las características de la base Syn utilizada, podemos establecer que si el tamaño en Mbytes para 1.000 individuos es de 192 Mbytes, para 35.000 individuos será de 6.720 Mbytes. Esto indica que la base de imágenes de toda la población carcelaria tiene un tamaño que permite almacenarla en un dispositivo estándar y económico disponible en el mercado.

Como trabajos futuros se pueden mencionar:

- El estudio de arquitectura e infraestructura de un “cerrojo biométrico”, que considere sistemas biométricos de tipo facial, de iris y huella dactilar.
- Estudio de algoritmo de procesamiento de imágenes utilizado para la obtención de la base Syn que permita realizar deformaciones sobre la imagen y así generar imágenes nuevas de los ojos de las personas privadas de su libertad. Esto generaría una base de imágenes que contemple una mayor cantidad de imágenes por persona con diferentes características. Esto permite preparar al sistema ante diferentes intentos de fraude.

## 8 Bibliografía

1. Xiaofu He, Pengfei Shi: Extraction of Complex Wavelet Features for Iris Recognition. In: 19th International Conference on Pattern Recognition. IEEE (2008).
2. Donald M. M., Soumyadip R., Dexin Z.: DCT-Based Iris Recognition. In: Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4 pp. 586—595. IEEE (2007).
3. Li M., Yunhong W., Tieniu T.: Iris Recognition Based on Multichannel Gabor Filtering. In: 5th Asian Conference on Computer Vision on Proceedings of the International Conference. Melbourne, Australia (2002).
4. Daugman J. G.: High Confidence Visual Recognition of Persons by a Test of Statistical Independence. In: Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148--1161. IEEE (1993).
5. CASIA Iris Image Database (Versión 4.0), <http://biometrics.idealtest.org/findDownloadDbByMode.do?mode=Iris>.
6. Gonzalez R. C., Woods R. E., Eddins S. L: Digital Image Processing, (2004)
7. Yet Another Wavelet Toolbox, <http://sites.uclouvain.be/ispgroup/yawtb/>
8. Daugman J.: How iris recognition works In: Transactions on Circuits and Systems for Video Technology, vol.14, no.1, pp.21-30. IEEE (2004).