Nuevos Algoritmos y Ataques a Sistemas de Identificación Biométrica basados en Reconocimiento de Iris

Alberto de Santos Sierra[1], Carmen Sánchez Ávila[2] y Vicente Jara Vera[3]

[1] Grupo de Biometría y Tratamiento Numérico de la Información.
Centro de Domótica Integral (CeDInt)
<alberto@cedint.upm.es>
[2] Grupo de Biometría y Tratamiento Numérico de la Información.
Centro de Domótica Integral (CeDInt)
<csa@mat.upm.es>
[3] Dpto. de Matemática Aplicada a las Tecnologías de la Información.
ETSI de Telecomunicación. Universidad Politécnica de Madrid.
Ciudad Universitaria s/n, 28040 Madrid
<vjara@mat.upm.es>

Resumen En este trabajo se recogen dos enfoques claramente definidos: Primeramente, se propone una mejora a los sistemas actuales de detección de iris, tanto en detección de pupila, como en detección de iris en sí misma. Dichos algoritmos rompen con el esquema clásico de aislamiento de iris, y proponen una nueva idea en este campo. Además, se utilizarán bases de datos actuales para la evaluación de los resultados. Por otro lado, se presenta un esquema de ataque a un sistema de iris en el que a partir del patrón biométrico se reproduce una imagen de iris capaz de confundir a dicho sistema, mediante la utilización de algoritmos genéticos. Este novedoso procedimiento, permitiría a un determinado usuario falsificar su identidad, utilizando simplemente el patrón biométrico de iris de otro usuario. Los resultados de este algoritmo muestran como esto es factible. Además, no existe en la literatura nada similar en cuestión de ataques de este tipo a un sistema de iris.

1. Introducción

El reconocimiento de iris posee diferentes etapas desde el momento en que la imagen es capturada por una cámara, hasta que el sistema es capaz de decidir si el usuario que está accediendo es en verdad quien dice ser, [5], [6], [10]. Estas etapan involucran primeramente un preprocesamiento de la imagen (detección de pupila, iris, párpados, pestañas, ...), extracción de características, procesamiento de las mismas, y comparación. Los algoritmos aquí presentados están más relacionados con el preprocesamiento de la imagen adquirida, concretamente con algoritmos de detección de pupila e iris. Dichos algoritmos, como se verá más adelante con detalle, están basados en morfología matemática, [8]. Por otro lado, los sistemas biométricos presumen de ser capaces de resistir ataques

tales como el acceso de un individuo que haga pasarse por otro usuario. Sin embargo, en sistemas basados en huella ya es posible crear una huella a partir de las minucias obtenidas, o almacenadas en una base de datos. Es decir, conociendo únicamente el patrón biométrico se puede obtener qué huella proporciona dicho patrón, [3]. Inspirado en los resultados obtenidos para huella, este trabajo propone un esquema similar en cuanto al concepto: Obtener una imagen de iris a partir de su patrón biométrico.

Para realizar esto, los algoritmos genéticos son propuestos como una útil herramienta, [1], [2], [7]. Puesto que el tiempo no es una cuestión importante cuando se intenta atacar a un sistema biométrico, sino que prima más la precisión con la que se obtenga el resultado requerido, el uso de los algoritmos genéticos queda por lo tanto justificado.

El documento comenzará por lo tanto tratando los algoritmos de detección de pupila y de iris, finalizando posteriormente con los ataques a estos sistemas biométricos, aportando las oportunas conclusiones y líneas futuras de investigación.

2. Detección de Pupila

El algoritmo de detección de pupila presenta dos nuevos conceptos que no han sido usados con anterioridad. La primera idea trata sobre la eliminación de los brillos en la pupila, algo muy común en imágenes de iris, a partir de la siguiente transformación presentada en la Ecuación 1

$$I'(x,y) = \cos\left(\frac{2\pi}{255} I(x,y)\right) \tag{1}$$

donde $I(x,y)$ es la imagen de iris a la que se quiere eliminar dicho efecto indeseable. Con esta transformación se consigue que aquellos valores cercanos a 255, i.e. colores cercanos al blanco (destellos en la pupila), y aquellos valores cercanos a 0, i.e. colores cercanos al negro (la pupila), posean la misma intensidad. Una vez que esto se consigue, se realizan operaciones morfológicas para eliminar pequeños detalles, y así aislar completamente la pupila, tras una detección de bordes y una umbralización. Es importante resaltar, que el posterior algoritmo de detección de iris basa parte de su fortaleza en una buena detección de pupila, y que además, no es necesario obtener toda la circunferencia que rodee a la pupila, si no únicamente unos pocos puntos.

Los resultados mostrados en la Figura 1 se corresponden con la base de datos Casia V3, [4].

Por otro lado, y continuando con lo relativo a la detección de pupila, se propone un algoritmo para la detección de ésta en bases de datos donde detectar la pupila require un esfuerzo mayor, como es el caso de la base de datos ICE, [9].

En este caso, se utiliza morfología matemática pero aplicada no a la imagen en sí, sino al resultado de dividir la imagen en sus bits correspondientes. Es decir, puesto que cada color está representado con 8 bits, intensidades desde 0 (negro)

Figura 1. (Izq) Imagen Original, (Centro) Resultado de la Transformación con el coseno, (Dch) Resultado de la Segmentación

hasta 255 (blanco), se irán formando capas de imágenes con los bits de cada pixel, desde el más significativo al menos significativo. Con esto se obtendrán 8 capas, cada una de ellas con diferente información sobre la imagen en sí misma. Tomando la capa correspondiente al segundo bit menos significativo, y aplicando posteriormente morfología matemática para hacer más preciso el resultado, se obtienen las imágenes en la Figura 2.

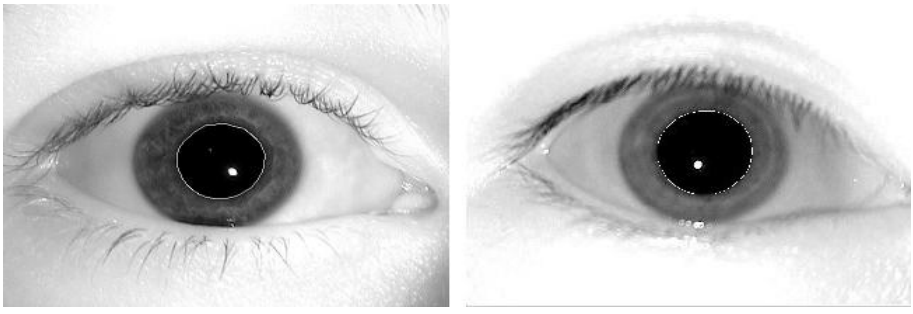

Figura 2. Resultados del procesamiento basado en mapa de bits en la base de datos ICE.

Finalmente, combinando ambos resultados se puede obtener un algoritmo potente de detección de pupila, para imágenes sencillas (versiones de CASIA v1), y para imágenes más complejas, como es la base de datos ICE.

Por último queda decir, que la detección de pupila quedará representada por la Figura 5, donde se puede apreciar que para representar la segmentación de pupila, únicamente hacen falta cinco puntos: dos horizontales, dos verticales y el centro.

3. Detección de Iris

Una vez que se ha detectado tanto los puntos importantes de la pupila como el centro, se procede a extraer el contorno del iris, o en su defecto, información suficiente para poder dilucidar en un posterior control de calidad, cómo de buena es la imagen, cómo de abierto está el ojo, si el ojo está desplazado, etc...

Estos puntos, pueden apreciarse en la Figura 5, donde se proporciona el resultado del algoritmo que se explica a continuación. Una vez obtenido el centro de la pupila (el centro de iris no será calculado, siendo ésta otra de las ventajas de este algoritmo), se centran tres distribuciones diferentes (ver Cuadro 1 y Figura 3), cuya finalidad es simplemente degradar (aclarar) aquellas componentes más alejadas de la pupila, dejando inalteradas aquellas componentes más cercanas al centro de la misma. Posteriormente, se aplica un filtro basado también en operadores morfológicos que se encarga de dejar pasar aquellas componentes más oscuras en una imagen.

Nombre	Expresión Matemática	Parámetros
Gaussiana	$A_\gamma e^{-\sigma_x(x-x_0)^2} e^{-\sigma_y(y-y_0)^2}$	A_γ, σ_x, σ_y, (x_0, y_0)
Coseno I	$A_I cos(x-x_0) cos(y-y_0)$	A_I, (x_0, y_0)
Coseno II	$A_{II} cos^2(x-x_0) cos^2(y-y_0)$	A_{II}, (x_0, y_0)

Cuadro 1. Descripción matemática de las distribuciones

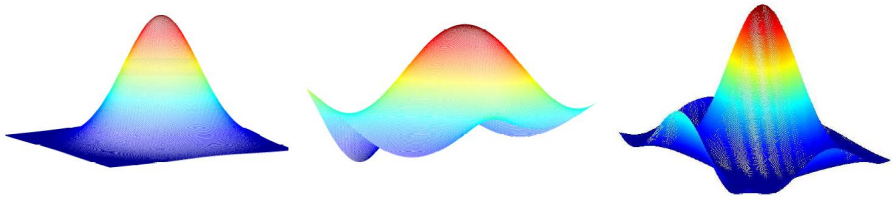

Figura 3. Distribuciones para degradar las imagenes de iris. Su forma hace que las componentes más alejadas a la pupila se vean atenuadas.

La combinación de estas distribuciones junto con el filtro permiten acotar completamente el iris, pero no dar un contorno que ajuste perfectamente el iris. Sin embargo, los puntos aportados por este algoritmo (puntos verticales y horizontales) proporcionan información más que suficiente para poder rechazar una imagen, y pedir otra captura, o por el contrario aceptarla, y continuar con el proceso de extracción de características.

El resultado de los diferentes filtros, puede apreciarse en la Figura 4, donde de izquierda a derecha y de arriba hacia abajo, se aprecia la imagen original, y los resultados provenientes de las distribuciones gaussianas, Coseno I y Coseno II, respectivamente.

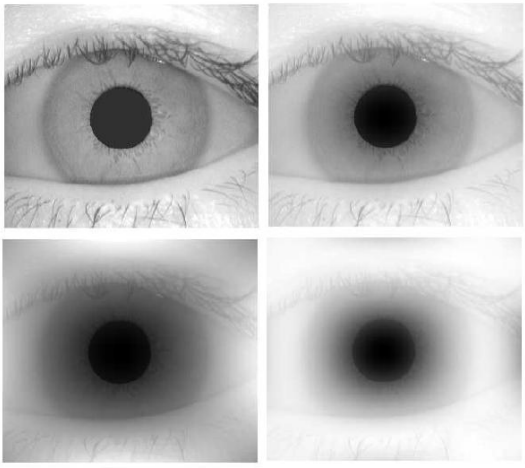

Figura 4. Resultado visual de las diferentes distribuciones

Por último, se presenta en la Figura 5, el resultado final de la segmentación, reuniendo no sólo la detección de iris, sino también la detección de pupila.

Finalmente, los parámetros de la distribución gaussiana (ver Cuadro 1) pueden controlarse y relacionarse de tal forma, que se pueda obtener una segmentación de iris tal y como ha sido siempre concebida, es decir, detectando completamente el iris en la imagen. Mediante una red neuronal que relacione σ_x y σ_y con las medidas obtenidas en una primera segmentación de iris, se obtienen los resultados ofrecidos en la Figura 6. Todos estos resultados se aprovechan del gran contraste de color existente entre el iris (siempre de algún color, a no ser que exista aniridia), y la esclera (parte blanca de los ojos).

Sin embargo, aunque pueda conseguirse esta resolución, con la segmentación ofrecida en la Figura 5 es suficiente, obteniendo resultados muy importantes no sólo en precisión a la hora de segmentar, sino en tiempos de procesamiento pues para realizar la detección de pupila y la detección de iris, únicamente emplea 2.2 segundos de media en realizar toda la segmentación.

4. Ataque a sistemas de iris

La idea de este ataque reside en el siguiente escenario: Sea un usuario $\mathcal{A}$ cuyo patrón biométrico es $\mathcal{T}_\mathcal{A}$. Sea ahora un usuario $\mathcal{B}$ que intenta acceder al sistema haciéndose pasar por $\mathcal{A}$, contando únicamente con $\mathcal{T}_\mathcal{A}$. El problema consiste en

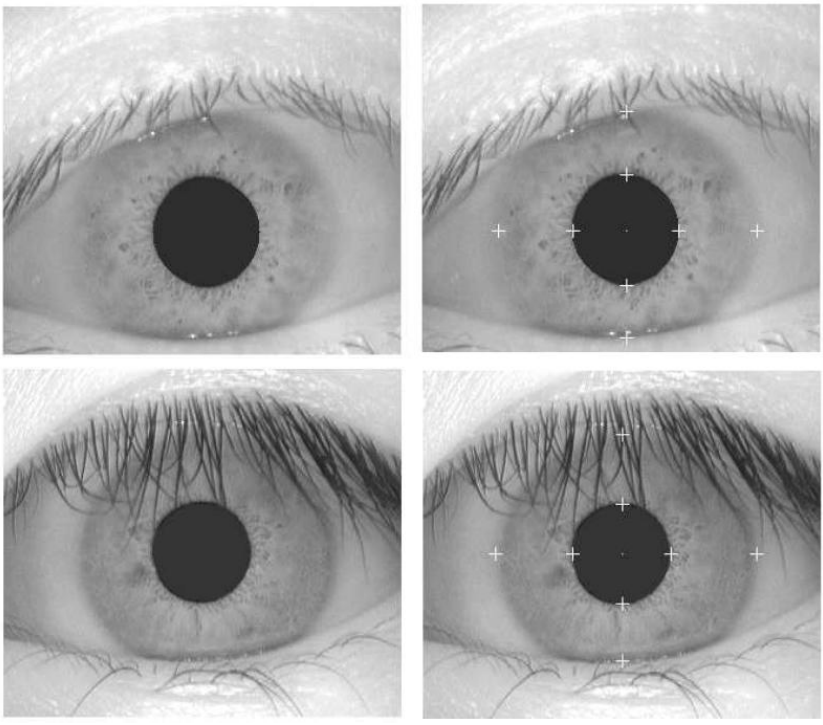

Figura 5. Resultado final de la segmentación

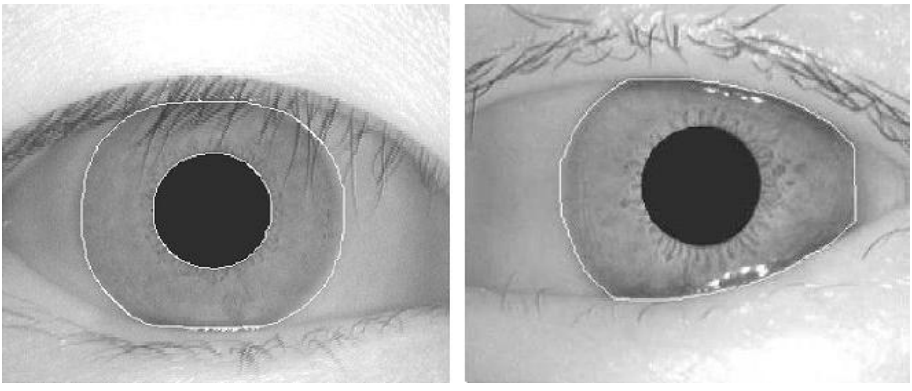

Figura 6. Segmentación clásica mediante este nuevo método

conseguir acceder al sistema a partir del patrón $\mathcal{T}_{\mathcal{A}}$ y con la imagen de iris de $\mathcal{B}$. Una vez que $\mathcal{B}$ ha conseguido una imagen de iris cuyo patrón de iris es $\mathcal{T}_{\mathcal{A}}$, el sistema será incapaz de distinguir entre $\mathcal{A}$ y $\mathcal{B}$. Para solventar dicho problema, se ha implementado un algoritmo genético capaz de transformar la imagen de ojo del usuario $\mathcal{B}$, de tal forma que su patrón, $\mathcal{T}_{\mathcal{B}}$, coincide tanto como se desee con el patrón a falsificar, $\mathcal{T}_{\mathcal{A}}$. Además, el patrón de iris es extraído utilizando una corona circular, y promediando de forma radial los valores de intensidades existentes a lo largo de la corona circular para todos los ángulos, [10].

Una vez presentado el problema, en la Figura 7 se aprecian los dos usuarios $\mathcal{A}$ y $\mathcal{B}$.

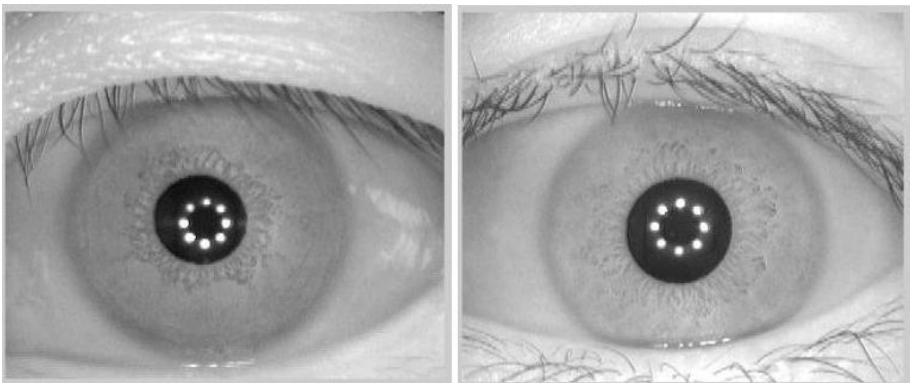

Figura 7. (Izq) Usuario $\mathcal{A}$, (Dch) Usuario $\mathcal{B}$

Además, en la Figura 8, se aprecia primeramente en el lado izquierdo el patrón biométrico de $\mathcal{A}$, es decir, $\mathcal{T}_{\mathcal{A}}$. En el centro, se aprecian diferentes ejecuciones del algoritmo genético, que se adapta perfectamente al patrón biométrico requerido. El algoritmo está diseñado de tal manera que $\mathcal{T}_{\mathcal{B}}$, puede ser tan parecido a $\mathcal{T}_{\mathcal{A}}$, como se desee. Incluso cabe la posibilidad de que sean iguales.

Sin embargo, en contra de parecer una buena idea, hacerlos iguales sería un error. Como puede apreciarse finalmente en la imagen de la derecha, para un mismo usuario existe una gran variación en el patrón biométrico para diferentes muestras. Por lo tanto, el algoritmo preve esta variabilidad, y una vez obtenida la solución, se distorsiona para que no parezca una copia exacta del patrón a falsificar.

Finalmente, en la Figura 9 puede apreciarse el resultado de la falsificación, y cómo la imagen del usuario $\mathcal{B}$ ha sido alterada de tal forma que ahora su patrón, $\mathcal{T}_{\mathcal{B}}$, es lo suficientemente similar a $\mathcal{T}_{\mathcal{A}}$, es decir el patrón de $\mathcal{A}$, como para engañar al sistema de identificación biométrica.

El sistema es incapaz de distinguir un usuario del otro, y por lo tanto, el usuario $\mathcal{B}$ ha conseguido acceder al sistema.

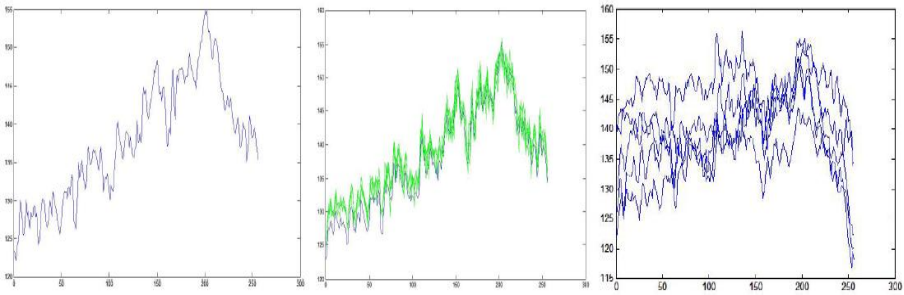

Figura 8. $\mathcal{T}_{\mathcal{A}}$, $\mathcal{T}_{\mathcal{A}}$ y resultados del algoritmo genético, $\mathcal{T}_{\mathcal{A}}$ para diferentes muestras de un mismo usuario $\mathcal{A}$.

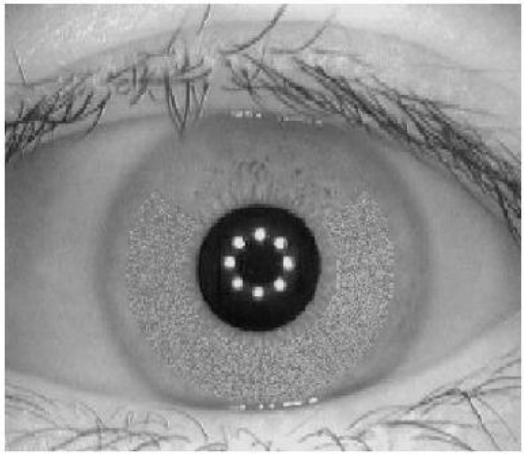

Figura 9. Resultado final del algoritmo: $\mathcal{B}$ cuyo patrón biométrico es $\mathcal{T}_{\mathcal{A}}$.

5. Conclusiones y Trabajo Futuro

En este trabajo se han presentado varios algoritmos tanto para la mejora de la detección de iris, y de pupila, como un posible ataque para que un determinado usuario acceda al sistema sin necesidad de pertenecer a dicho sistema.

Respecto a los algoritmos de segmentación, se propone un nuevo preprocesado basado íntegramente en morfología matemática y distribuciones matemáticas, que hacen más precisa la detección de iris y de pupila. La rapidez con la que estos algoritmos llevan a cabo sus tareas aventajan en gran medida a algunos algoritmos actuales, pues los algoritmos aquí presentados aún no han sido optimizados ni implementados en un dispositivo específico, es decir, fuera de un PC.

Respecto al ataque al sistema biométrico, sería bueno camuflar de alguna manera la modificación hecha al usuario que quiere falsificar la entrada, pues a primera vista se ve como ese iris es un tanto diferente de uno normal, aunque el sistema de reconocimiento sea incapaz de diferenciarlos. Se podrían poner más restricciones al algoritmo genético para que pudiera darle un aspecto más parecido al de un iris humano, o usar autómatas celulares para obtener dicho requisito.

Sin embargo, los avances alcanzados tanto en segmentación como en el ataque al sistema de iris (el primero de este tipo que se ha hecho en la literatura), son bastante buenos y sobre todo prometedores.

6. Agradecimientos

Los autores quieren agradecer al proyecto CENIT Segur@: Seguridad y Confianza en la Sociedad de la Información, financiado por el Ministerio de Industria, Turismo y Comercio.

Referencias

[1] T. Bäck, D. B. Fogel, Z. Michalewicz, Eds. *Evolutionary Computation 1: Basic Algorithms and Operators.*, Institute of Physics Publishing, Bristol, 2000.

[2] T. Bäck, D. B. Fogel, Z. Michalewicz, Eds. *Evolutionary Computation 2: Advanced Algorithms and Operators.*, Institute of Physics Publishing, Bristol, 2000.

[3] R. Capelli, A. Lumini, D. Maio and D. Maltoni, *'Can Fingerprints be reconstructed from ISO Templates?'*, in Proc. *International Conference on Control, Automation, Robotics and Vision (ICARCV2006)*, Singapure, December 2006.

[4] CASIA Iris Image Database. http://www.sinobiometrics.com

[5] J. Daugman, *High Confidence Visual Recognition of Persons by a Test of Statistical Independence*, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No 11, Nov. 1993.

[6] J. Daugman, *'How Iris Recognition Works'*, IEEE Transactions on Circuits and Systems For Video Technology, Vol. 14, n 1, January 2004.

[7] A. E. Eiben and J. E. Smith, *Introduction to Evolutionary Computing*, Berlin, Germany: Springer, 2003.

[8] R. C. González, R. E. Woods, S. L. Eddins, *Digital Image Processing*, 2^{nd} Edn, Prentice All, 2004.
[9] Iris Challenge Evaluation http://iris.nist.gov/ICE/
[10] A. de Santos Sierra, C. Sánchez Ávila, E. Marchiori, *Iris Recognition: Segmentation enhancement by using Morphological Operators*, Master Final Tesis, June, 2007. Amsterdam.