Detección de Muestras Inválidas en Sistemas de Autenticación Basados en Geometría de la Mano

Javier Burgues, Julian Fierrez, Daniel Ramos,
Maria Puertas, and Javier Ortega-Garcia

Grupo de Reconocimiento Biométrico - ATVS, EPS - Univ. Autonoma de Madrid
C/ Francisco Tomas y Valiente, 11 - Campus de Cantoblanco - 28049 Madrid, España
{javier.burgues,julian.fierrez,daniel.ramos,
maria.puertas,javier.ortega}@uam.es
http://atvs.ii.uam.es

Resumen El rendimiento de un sistema de autentificación basado en geometría de la mano depende fuertemente de la calidad de las imágenes capturadas. Factores relacionados con el dispositivo de adquisición (p.ej. superficie del escáner sucia) o el proceso de interacción entre el usuario y el sensor (p.ej. posicionamiento de la mano) pueden deteriorar la calidad de la muestra adquirida. Por lo tanto, después de capturar una muestra es importante evaluar su validez. En este trabajo, se presenta un módulo para detectar imágenes inválidas a partir de medidas geométricas. La organización de los experimentos consiste en un sistema de verificación basado en geometría de la mano que es probado en dos diferentes escenarios de adquisición: BiosecurID (400 usuarios, escáner) y Biosecure (210 usuarios, cámara). Los resultados confirman una notable mejora en el rendimiento del sistema a medida que el porcentaje de muestras inválidas rechazadas aumenta. En concreto, un descarte de aproximadamente el 5 % de las imágenes en BiosecurID produce una mejora del 2.8 % EER al 0.1 % EER.

Keywords: Biometría, geometría de la mano, calidad, muestras inválidas

1. Introducción

La autentificación de personas en nuestra interconectada sociedad de la información se está convirtiendo en un asunto decisivo. La biometría consiste en identificar a una persona a través de sus rasgos fisiológicos o comportamentales (huella dactilar, firma, iris, geometría de la mano, etc.) y proporciona más seguridad y comfort que los métodos de autentificación convencionales, que dependen de lo que sabes (como un password) o de lo que tienes (como una tarjeta identificativa) [1].

Para muchas aplicaciones de control de acceso, en las cuales la aceptación por parte del usuario es un factor importante, la huella dactilar y el iris pueden no ser adecuadas para la protección de la privacidad del individuo. En esas situaciones, los sistemas de identificación basados en mano, caracterizados por su recopilación de datos de modo no intrusivo, juegan un papel importante.

Dos tipos de indicadores biométricos pueden ser extraidos de las imágenes de la mano: rasgos de la huella palmar (lineas principales, arrugas, minucias, etc.) y carac-

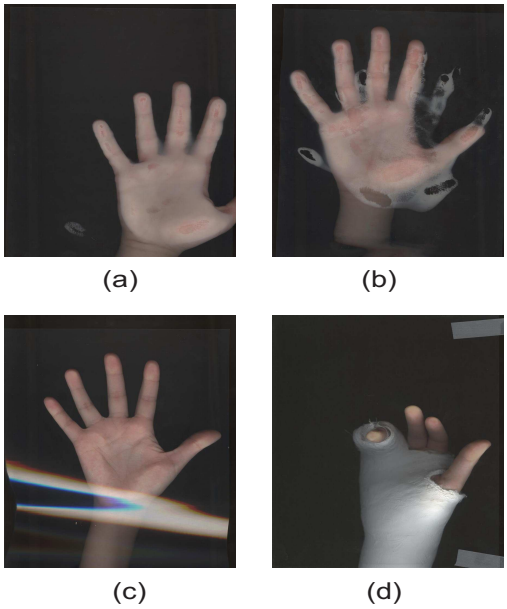

Figura 1: Ejemplos de imágenes inválidas

terísticas geométricas (p.ej. longitud y anchura de los dedos). Nosotros nos hemos centrado en el segundo tipo debido a su simplicidad. En la literatura, se han considerado muchos sistemas diferentes de reconocimiento basado en geometría de la mano [2,3,4]. Por ejemplo, en [2] se presenta un sistema basado en varias anchuras, alturas, desviaciones y ángulos de los dedos. El trabajo descrito en [3] trata los dedos individualmente rotándolos y separándolos de la mano. Oden et al. [4] usa la forma de los dedos representada con poliniomios implícitos de cuarto grado.

Las imágenes de la mano son, generalmente, obtenidas mediante un escáner o una cámara. En el primer caso, las imágenes escaneadas pueden presentar ruido debido a humedad presente en la superficie del escáner (debido a manos mojadas), reflejos de luz, deformación de los dedos (excesiva presión del usuario sobre la superficie), etc. En imágenes procedentes de una cámara, el mayor problema viene determinado por la sombra que proyecta la mano sobre el fondo debido a la iluminación. Estas condiciones, a su vez, afectan a la calidad de las imágenes adquiridas (ver Fig. 1). Las muestras de baja calidad incrementan la tasa de falso rechazo del sistema (FRR), y por consiguiente reducen la tasa de aceptación positiva (TAR). Estos errores imposibilitan el acceso a información o instalaciones a personas autorizadas. Por consiguiente, en sistemas de adquisición no supervisados es deseable detectar las muestras defectuosas para poder solicitar nueva información válida.
La arquitectura típica de un sistema automático de verificación basado en mano se muestra en la Fig. 2. Como se ha mencionado antes, el presente trabajo está centrado en geometría de la mano. En particular, se estudia el problema de la detección de

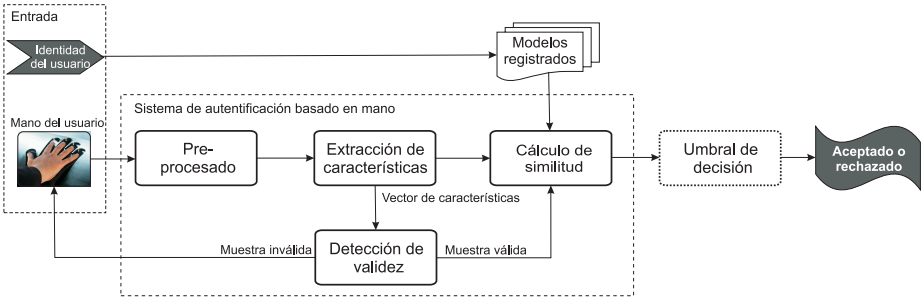

Figura 2: Arquitectura de un sistema de verificación basado en mano

muestras inválidas en sistemas de geometría de mano. Para una numerosa población, se realiza un análisis de las proporciones geométricas presentes en la mano con el objetivo de definir algunas constantes válidas anatómicamente. Para una imagen de entrada, se comprueban las constantes resultantes y así se determina su validez. El resto del artículo se estructura del siguiente modo. En la sección 2 resumimos los conceptos principales para trabajar con muestras inválidas en sistemas biométricos. La sección 3 explica las constantes geométricas usadas en la etapa de detección de validez. La configuración de los experimentos y los resultados obtenidos son explicados en las secciones 4 y 5, respectivamente. Finalmente, algunas importantes conclusiones son resaltadas en la sección 6, junto con el trabajo futuro.

2. Modos de trabajar con muestras inválidas en sistemas biométricos

La baja calidad en los datos es responsable de la mayoría de errores de correspondencia en los sitemas biométricos y puede ser la mayor debilidad de algunas implementaciones. El impacto de la información de baja calidad puede ser reducido de varios modos, muchos de los cuáles dependen de métodos efectivos para medir automáticamente la calidad de los datos. Basándonos en la calidad medida, podemos invocar diferentes algoritmos de procesamiento, o podemos rechazar la señal adquirida. En este caso, deberemos tener definido un procedimiento excepcional para aquellos usuarios que sus muestras sean rechazadas por el algoritmo de medida de calidad. A continuación se describen tres procedimientos operativos para tratar con imágenes de baja calidad:

- **Readquisición**: Para mejorar la calidad de la muestra final capturada es posible adquirir tantas muestras como sean necesarias para satisfacer un criterio de validez. Sin embargo, un bucle de re-captura muy persistente puede incomodar al usuario por lo que una implementación típica es una política de “hasta tres intentos”. Esto depende de las especificaciones de la aplicación, donde puede ser obligatorio procesar la primera muestra adquirida sin tener en cuenta su calidad. Para evitar la readquisición, algunos sistemas escogen la mejor señal de un conjunto capturado mientras el ususario interactúa con el sensor.

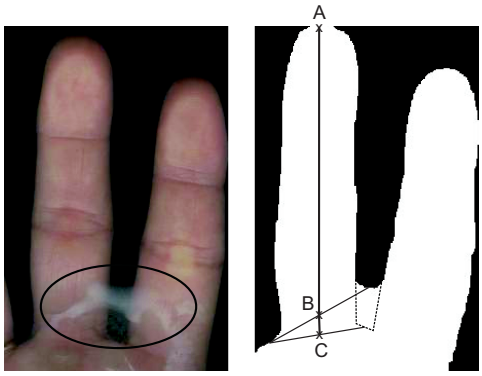

Figura 3: Ejemplo de una imagen inválida

- **Procesamiento basado en calidad**: Los algoritmos de medida de calidad pueden ser utilizados para adaptar los procesos del sistema adecuadamente. En la fase de pre-procesado, un sistema de identificación detecta la calidad e intenta mejorar la imagen y extraer características más robustas al tipo de degradación que está sufriendo la señal biométrica. Dependiendo de la calidad de las plantillas adquiridas, se pueden usar diferentes algoritmos de similitud o ajustar el umbral de decisión para dar más importancia a las características de alta calidad.
- **Intervención humana**: La última opción para sistemas que no incorporan procesamiento basado en calidad es recurrir a la intervención humana para realizar un proceso alternativo de reconocimiento.

En este trabajo, sólo distinguiremos entre imágenes de alta calidad o baja calidad, descartando las últimas. Como se verá en los experimentos, siempre existe un compromiso entre la tasa de error del sistema y el número de muestras rechazadas. Si se desea reducir el EER, deberemos ser muy restrictivos en la calidad de las imágenes y, por lo tanto, descartar un gran número de muestras. Dependiendo de la aplicación, la principal restricción podría ser minimizar el EER, la tasa de rechazo de usuarios o mantener un equilibrio entre estas dos variables. Por ejemplo, en una aplicación de baja seguridad, puede ser tolerado un error grande por lo que podemos reducir la tasa de rechazo de usuarios con el fin de minimizar las molestias al usuario.

3. Definición de las constantes geométricas

Debido a problemas en la etapa de adquisición, pueden obtenerse imágenes de baja calidad. Por ejemplo, un problema típico es la presencia de humedad en la superficie del escáner (ver Fig. 3a). Debido a esto, el contorno extraído de la imagen de entrada puede no representar correctamente la mano del usuario (ver Fig. 3b). En este ejemplo, la longitud del dedo corazón será calculada como el segmento AB, siendo su longitud

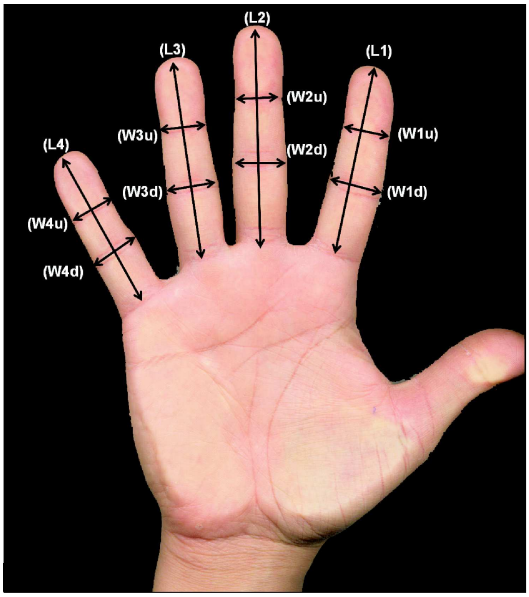

Figura 4: Conjunto de características

real el segmento AC. Por lo tanto, debido a la baja calidad de la imagen se ha introducido un error (segmento BC) en la medida de longitud, que deteriorará el rendimiento del sistema. Nuestra propuesta es detectar este tipo de imágenes fijándose en las relaciones entre las longitudes de los dedos. En general, el cuerpo humano conserva ciertas proporciones (p.ej. la longitud de la mano es aproximadamente la décima parte de la altura de un hombre). Experimentalmente, hemos medido los cocientes entre varias parejas de longitudes de dedos en un conjunto grande de muestras y hemos observado que esos cocientes son prácticamente constantes. Este hecho propicia que cada cociente pueda ser modelado por una función Gaussiana de media μ y desviación típica σ.

3.1. Medidas geométricas

Nuestro principal problema son los artefactos entre los dedos en la imagen de entrada que producen un contorno similar al de una muestra sin dichos artefactos, como se observa en el ejemplo de la Fig. 3. Por esta razón, definimos tres cocientes entre longitudes de dedos que pueden ayudarnos a decidir si las proporciones de la mano actual no son anátomicamente correctas (ver Fig. 4):

$$r_1 = L3/L4 \tag{1}$$

$$r_2 = L2/L3 \tag{2}$$

$$r_3 = L2/L1 \tag{3}$$

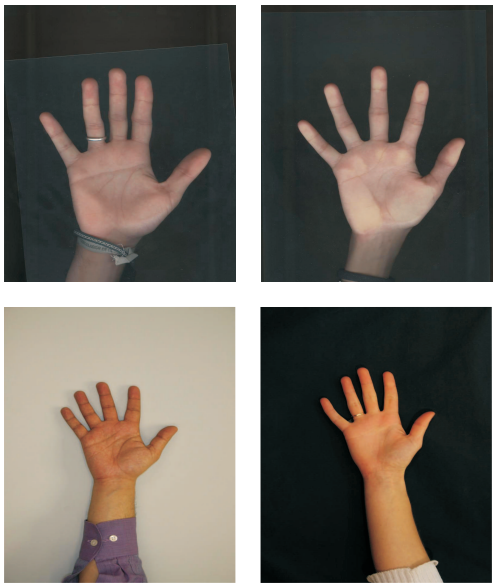

Figura 5: Ejemplos de imágenes válidas. Arriba: Base de datos BiosecurID, Abajo: Base de datos Biosecure

3.2. Detección de las muestras inválidas

Supongamos que hemos calculado los parámetros μ y σ que modelan cada uno de las relaciones r_1 a r_3 explicadas en la sección anterior. Para una imagen de entrada, examinamos su vector de características y calculamos sus cocientes entre longitudes de los dedos. Si cada cociente está dentro del rango $[\mu - k\sigma, \mu + k\sigma]$, donde k es un parámetro modificable, la muestra actual es aceptada. En caso contrario, consideramos que la muestra es inválida y alguno de los procedimientos explicados en la sección. 2 debe ser invocado.

4. Configuración experimental

Para los experimentos, se usarán los subconjuntos de mano de dos bases de datos biométricas multimodales BiosecurID [5] y Biosecure [6]. Nuestro propio sistema de autentificación basado en geometría de la mano [7] será probado sobre estos dos escenarios diferentes.

Escenario 1: BiosecurID. Esta base de datos comprende un total de 12.800 imágenes de mano diferentes provenientes de 400 usuarios $\times$ 2 manos $\times$ 4 sesiones $\times$ 4 muestras. Las imágenes en color han sido obtenidas utilizando un escáner de escritorio (ver

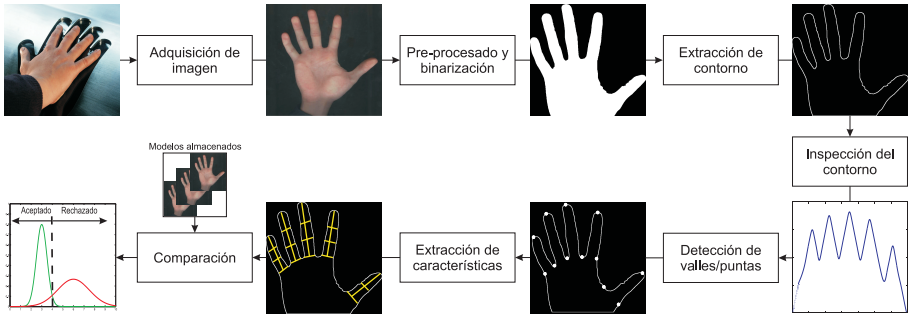

Figura 6: Descripción del sistema

ejemplos en Fig. 5 (arriba)). Por sencillez, antes del pre-procesado, las imágenes se convierten a escala de grises. Las muestras de las dos primeras sesiones (8 por usuario) son usadas para calcular los modelos de usuario, sólo para las manos derechas.

Escenario 2: Biosecure. Esta base de datos está compuesta por 210 usuarios, 2 sesiones y 4 imágenes por sesión. En este caso, las imágenes en color han sido capturadas usando una cámara y, debido al fondo no uniforme, se aplican ténicas de segmentación basadas en color. Un modelo de usuario se construye con las 4 muestras de la primera sesión. Se muestran algunos ejemplos de imágenes en la Fig. 5 (abajo).

Las puntuaciones de impostor se obtienen mediante la comparación del modelo de usuario con una muestra de mano (la primera disponible en las sesiones que no han sido utilizadas para extraer el modelo de usuario) de todos los usuarios restantes. Las puntuaciones genuinas se calculan comparando las últimas muestras disponibles de un usuario con su propio modelo.

Los experimentos se estructuran de la siguiente manera: primero, se lleva a cabo una caracterización estadística de las constantes geométricas sobre la base de datos BiosecurID. A continuación, para ambos escenarios, se estudia la evolución del rendimiento en tareas de verificación a medida que el porcentaje de muestras rechazadas varía.

4.1. Descripción del sistema

La arquitectura global de nuestro sistema se muestra en la Fig. 6. La primera etapa es un módulo de extracción de contorno de la mano, a partir de la cual se obtiene la silueta de la mano. Luego, se calcula la distancia radial entre una referencia fija y el contorno de la mano para encontrar las coordenadas de las puntas y valles de todos los dedos. A continuación, se calculan algunas medidas basadas en distancia considerando estos puntos de referencia para construir el vector de características de las manos. El conjunto de características usado en la implementación del sistema se detalla en [7] y se resume en la Fig. 4. Finalmente, la similitud entre las manos registradas y de test se basa en una medida de distancia entre sus vectores de características.

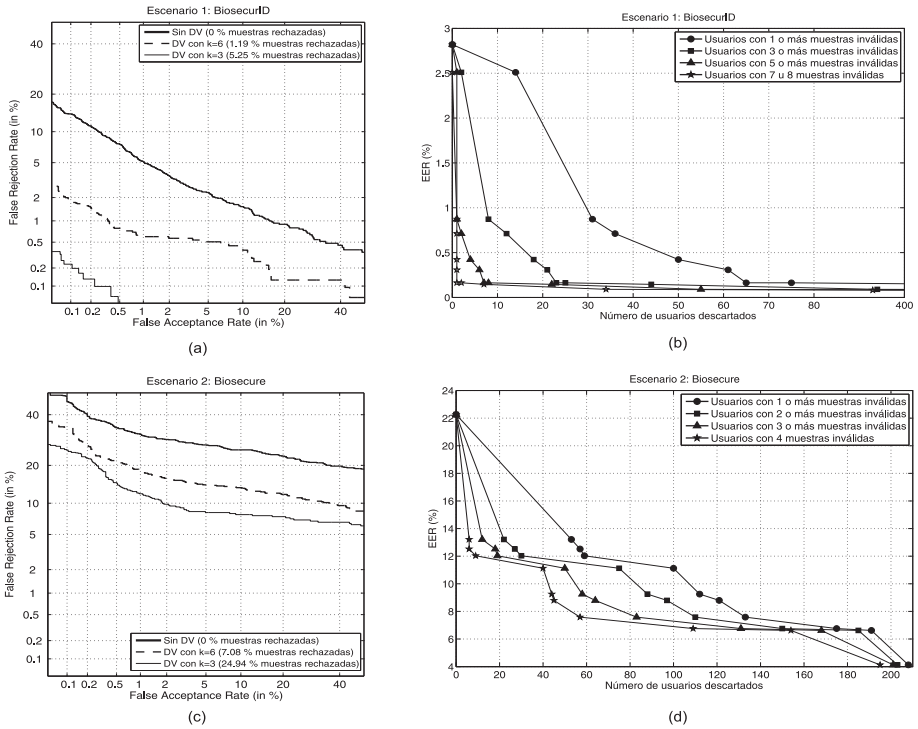

Figura 7: Resultados obtenidos en BiosecurID y Biosecure.

5. Resultados

En las siguientes secciones primero explicamos como hemos modelado las constantes geométricas. Después, estudiamos el rendimiento del sistema para diferentes rangos de validez definidos por la fórmula

$$\mu - k\sigma < r_i < \mu + k\sigma \tag{4}$$

para $i = 1, 2, 3$ donde r_i son las relaciones explicadas en la Sec. 3.1 y k controla la anchura del rango de aceptación (ver Sec. 3.2). Los rendimientos globales del sistema se muestran por medio de curvas DET.

5.1. Caracterización de las constantes geométricas

Los parámetros que modelan las constantes geométricas deberían ser, preferiblemente, extraídos de imágenes bien segmentadas. En consecuencia, las muestras involucradas en las puntuaciones genuinas más bajas (nuestro sistema está basado en una medida de disimilitud por lo que las puntuaciones genuinas bajas correponden a una alta similitud entre usuarios) se seleccionan para este propósito. Para cada imagen, se

Medida geométrica	μ	σ
r_1	1,2894	0,0564
r_2	1,0676	0,0256
r_3	1,1103	0,0349

Cuadro 1: Parámetros del modelo de caracterización

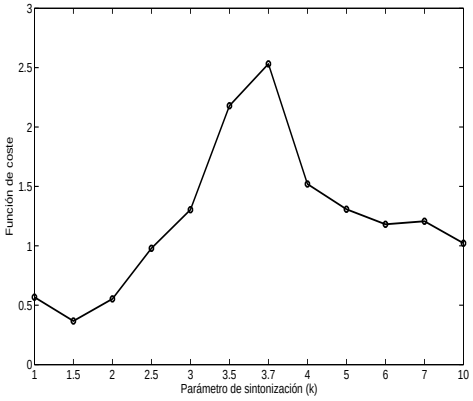

Figura 8: Ejemplo de compromiso entre error y porcentaje de rechazo

calculan los tres cocientes descritos en la Sec. 3.1 y, finalmente, se obtiene la media y desviación estándar de cada relación. El Cuadro 1 muestra el resultado.

5.2. Evaluación del rendimiento

En la Fig. 7 (izq.) se muestra, para ambos escenarios, el rendimiento en verificación usando diferentes configuraciones. En concreto, se muestran los resultados para tres situaciones: sin detección de validez (Sin DV) y con detección de validez (DV) para $k = 6$ y $k = 3$. Se puede observar que, en los dos escenarios, el rendimiento crece a medida que se descartan más muestras inválidas. Mientras que en BiosecurID la tasa de error del sistema puede ser reducida desde el 3 % hasta el 0.15 %, en Biosecure la mejora de rendimiento es menos significativa (desde el 22 % hasta el 8 %). En la Fig. 7 (der.) mostramos el EER según rechazamos usuarios con un número creciente de muestras inválidas. Para BiosecurID (Fig. 7b), podemos observar que las muestras inválidas más dañinas están concentradas en sólo dos o tres usuarios y, cuando estos usuarios son rechazados, el EER mejora desde el 2.8 % al 0.2 %. Por otro lado, Fig. 7d muestra que, en el segundo escenario, la mayoria de los usuarios tienen muestras que no cumplen nuestro criterio de validez porque para reducir el error al 50 %, al menos es necesario rechazar el 20 % de los usuarios. Esto puede ser debido al fondo no uniforme que dificulta la segmentación de las imágenes en el segundo caso. Además, la gran diferencia de rendimiento observada entre los dos escenarios (Fig. 7a vs. Fig. 7c) puede ser una consecuencia del mismo factor.

Estos resultados demuestran la utilidad del módulo de detección de validez.
Si consideramos una aplicación práctica, donde el rendmiento del sistema puede ser tan importante como la comodidad del usuario, el parámetro k puede ser ajustado para equilibrar el EER y el porcentaje de muestras rechazadas. Por ejemplo, la Fig. 8 muestra el valor óptimo de k, para la base de datos BiosecurID, que maximiza la función

$$f = \frac{1}{EER \times Rechazo} \tag{5}$$

donde EER significa Equal Error Rate y $Rechazo$ es el porcentaje de muestras rechazadas. En este ejemplo, la combinación óptima se alcanza para $k = 3.7$, lo que produce un EER del 0.16 % y una tasa de rechazo del 2.25 %.

6. Conclusiones

Se ha estudiado el problema de la detección de muestras inválidas en sistemas de verificación basados en geometría de la mano. Los experimentos de rendimiento han sido llevados a cabo en dos escenarios de adquisición diferentes (BiosecurID, basado en escáner y Biosecure, basado en cámara). En ambos casos, se ha observado una importante mejora en el rendimiento cuando se detectan y descartan las muestras defectuosas. Sin embargo, mientras que en el primer escenario un 0.5 % de los usuarios concentran las muestras inválidas, en el segundo dichas muestras están más uniformemente distribuidas. El módulo de detección de validez propuesto tiene un parámetro modificable (k) que controla el EER a costa de aumentar/reducir la tasa de rechazo de usuarios. El trabajo futuro incluye el estudio de medidas de calidad cuantitativas con el objetivo de añadir procesamiento basado en calidad en los sistemas de verificación basados en geometría de la mano.

7. Agradecimientos

Este trabajo ha sido financiado por los proyectos Bio-Challenge (TEC2009-11186) y BBfor2 (FP7 ITN-2009-238803), la Dirección General de la Guardia Civil, y la Cátedra UAM-Telefónica.

Referencias

1. A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Techn.*, vol. 14, no. 1, pp. 4–20, 2004.
2. R. Sánchez-Reillo, C. Sanchez-Avila, and A. González-Marcos, "Biometric identification through hand geometry measurements," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 22, no. 10, pp. 1168–1171, 2000.
3. E. Yörük, E. Konukoglu, B. Sankur, and J. Darbon, "Shape-based hand recognition," *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 1803–1815, 2006.
4. C. Öden, A. Erçil, and B. Büke, "Combining implicit polynomials and geometric features for hand recognition," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2145–2152, 2003.
5. J. Fierrez, J. Galbally, J. Ortega-Garcia, *et al.*, "Biosecurid: A multimodal biometric database," *Pattern Analysis and Applications*, 2010. to appear.
6. J.Ortega-Garcia, J.Fierrez, F.Alonso-Fernandez, *et al.*, "The multi-scenario multi-environment biosecure multimodal database (BMDB)," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2010. to appear.
7. J. Burgues, J. Fierrez, D. Ramos, and J. Ortega-Garcia, "Comparison of distance-based features for hand geometry authentication," in *Springer LNCS*, vol. 5707, pp. 325–332, 2009.