UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA
Escuela Técnica Superior de Ingenieros
de Telecomunicación

Autenticación de personas a partir de la biometría de la región dígito palmar

Jia Li Zai Jian

Escuela Técnica Superior de Ingenieros de Telecomunicación
Universidad de Las Palmas de Gran Canaria

Resumen. En este proyecto fin de carrera se ha desarrollado un sistema capaz de identificar personas a partir de la imagen de la región digito palmar. Las imágenes de las huellas adquiridas con una cámara digital comercial son procesadas mediante una serie de técnicas que mejora la calidad de las mismas para obtener un vector de características que contiene las minucias de la mencionada huella. A partir de esta plantilla es posible con un clasificador basado en semejanzas verificar la identidad del usuario con una fiabilidad del 98,33% y en un tiempo medio de 2s.

1. Introducción

Con el avance de la tecnología, cada día son más las tareas que antes eran realizadas por las personas, y ahora son realizadas de forma automatizada. Dentro del amplio abanico de posibilidades que nos brinda el desarrollo e innovación tecnológica, se ha observado que los sistemas de autenticación de personas se están convirtiendo en un área emergente [1], y consecuentemente, la biometría se sitúa como el foco de atención de los investigadores de estos sistemas.

La biometría puede definirse formalmente como la ciencia que se dedica a la identificación de personas a partir de unos rasgos de comportamiento o anatómico. Un ejemplo del rasgo de comportamiento es la firma, y por otro lado, ejemplos anatómicos los podemos encontrar en huellas dactilares, iris, etc.

Para que un sistema biométrico sea eficiente, los indicadores o rasgos personales objeto de estudio deben reunir las siguientes cualidades [2]:

- Permanencia: la característica no debe cambiar con el tiempo, o hacerlo muy lentamente.
- Unicidad: la existencia de dos personas con una característica idéntica debe tener una probabilidad muy pequeña;
- Universalidad: cualquier persona debe poseer esa característica;
- Cuantificación: la característica puede ser medida en forma cuantitativa.

El indicador biométrico de la mano, más conocido, que satisface los cuatros requisitos anteriormente señalados es la huella dactilar. Este indicador ha sido utilizado por los seres humanos para la autenticación personal hace más de cien años [3]. En la actualidad estas huellas representan una de las tecnologías biométricas más maduras y son consideradas pruebas legítimas de evidencia criminal en cualquier parte del mundo. Además, las aplicaciones relacionadas con las huellas no sólo se centran en la criminología, como identificación de sospechosos, huellas dejadas en un escenario de crimen…, sino también en el ámbito comercial,

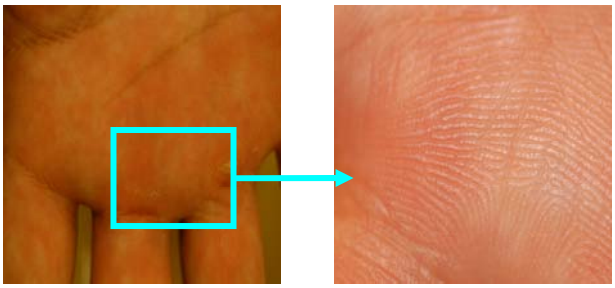


Figura 1. El cuadro marca la zona de la mano bajo estudio para el reconocimiento de personas

como control de acceso, sistema de seguridad, sistema de vigilancia…

Y siguiendo con esa línea de investigación e innovación, este proyecto presenta un novedoso sistema de autenticación basado en las huellas de la región dígito palmar de la mano es decir, la región de la palma de la mano comprendido entre los pliegues de flexión (de la base de los dedos) y el pliegue inferior (comúnmente conocido como la línea del corazón), como se observa en la figura 1, y que no ha sido utilizado en ningún sistema de este tipo conocido por nosotros. Adicionalmente se ha desarrollado un prototipo capaz de identificar personas en tiempo real con buenas prestaciones en rendimiento y eficiencia.

2. Objetivos

El reto de este proyecto de fin de carrera consiste en el desarrollo de un algoritmo para el reconocimiento de personas a través de las imágenes de la región dígito palmar de la mano. Por consiguiente, se pretende desarrollar un sistema de autenticación rápido, de bajo coste computacional, y con buena tolerancia de imágenes de huellas dañadas.

En resumen, los hitos u objetivos principales del presente proyecto son:

- Preparar los medios materiales para obtener las imágenes que conforman una base de datos, con el que se realizará dicho proyecto, por ejemplo, la fabricación de un soporte físico para el sensor de huellas, de modo que se puede lograr un cierto nivel de "automatización", y así conseguir un mayor grado de agilidad en la captura de huellas para la base de datos.
- Confeccionar una base de datos.
- Desarrollar algoritmos que sean capaces de llevar acabo los diversos trabajos que conlleva el proceso de autenticación, basándose en las muestras de la base de datos previamente preparadas.

3. Metodología

La comparación directa entre la imagen de la huella a ser identificada y las numerosas imágenes almacenadas en una base de datos, no servirían para una comparación confiable, debido a su alta sensitividad a los errores (por ejemplo: ruidos en la imagen, áreas de la huella dañada, o diferentes posiciones en la postura de la mano, ángulos de orientación o deformación del palma durante el proceso de toma de imagen).

Una solución avanzada a este problema es extraer unos puntos característicos (minucias) a partir de la imagen de la huella, y comparar entre estos conjuntos de características. Esta solución requiere de sofisticados algoritmos para el procesamiento de la imagen de la huella, eliminación del ruido, extracción de puntos característicos, tolerancia a rotación y traslación, etc. Al mismo tiempo, los algoritmos deben ser tan rápidos y eficientes como sea posible para garantizar su uso en aplicaciones con alta demanda.

En la figura 2 se puede ver un esquema del proceso completo. Las etapas más importantes consisten en: la adquisición de imagen de la huella, pre-procesamiento o mejora de la imagen, extracción de puntos característicos para la creación de plantillas específicos para cada usuario, en la cual contiene la información para la identificación, y el proceso de identificación.

3.1 Adquisición de las imágenes

Las imágenes de las huellas fueron adquiridas con una cámara digital con la resolución máxima

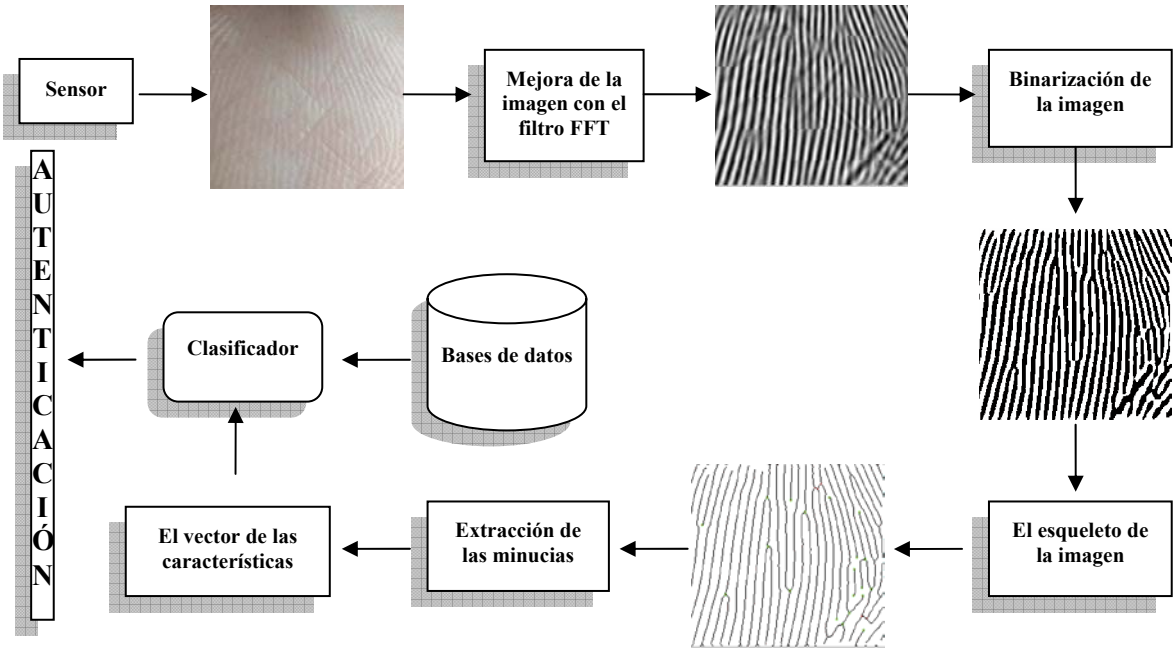


Figura 2. Diagrama de bloques de los pasos del proceso de reconocimiento

de 1,5 Mega-píxeles, situado sobre un soporte construido específicamente para este proyecto. De forma que, se ha confeccionado una base de datos con 14 fotos de 38 personas diferentes, esto es, un total de 532 imágenes. De las 14 fotos de cada persona, 5 serán utilizadas para entrenar los parámetros del sistema, es decir, son las plantillas de referencia del usuario, y las 9 restantes para la fase de verificación.

3.2 Pre-procesado de la imagen

Con esta etapa se pretende mejorar la calidad de la imagen eliminando ruidos, subsanando cortes, resaltando los relieves de la huella, etc. El principio básico de funcionamiento de la técnica utilizada es, dividir la imagen en bloques (32x32 píxeles), y a continuación, se filtra cada bloque con un filtro específico, creado previamente y basado en la dirección predominante de cada bloque [4].

Este filtro tiene la propiedad de resaltar las líneas en la dirección predominante del bloque objeto de estudio, y se consigue mediante la magnitud de la transformada de Fourier del propio bloque elevado a una constante 'k' [5].

Para eliminar el efecto borde que surge en todo procesado digital de imágenes por bloques, se optó por filtrar paso bajo la imagen obtenida, mediante una máscara de 3x3. Este método es poco costoso en tiempo de cálculo y con unos resultados bastante buenos.

3.3 El esqueleto de la imagen

A partir de la imagen pre-procesada y filtrada es posible binarizarla con un umbral, en este caso calculado mediante el método de Otsu, y una vez obtenida la imagen en blanco y negro se esqueletiza, esto es, todas las líneas de la imagen se adelgazan a una anchura igual a 1 píxel. Entre las diferentes técnica de esqueletización, considerando el tiempo de ejecución y calidad del esqueleto, se decidió utilizar la técnica de adelgazamiento basada en operaciones morfológicas [6] [7], que consiste en ir erosionando los píxeles de la borde de las estructuras de la imagen, hasta conseguir el esqueleto de la imagen.

3.4 Extracción de las minucias

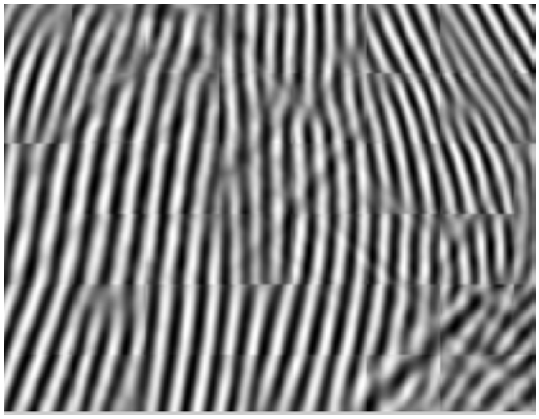
En una huella se encuentran diferentes tipos de minucias, pero las más utilizadas son las terminaciones y bifurcaciones. Naturalmente, para poder identificar a una persona mediante las minucias de su huella es necesario poder representar a éstas últimas para poder compararlas. La representación estándar consiste en asignar a cada minucia: su posición espacial

(x, y) y, su dirección *θ,* que es tomada con respecto al eje *x*, en el sentido contrario a las agujas del reloj [8]; evidentemente, existen muchas más representaciones posibles…

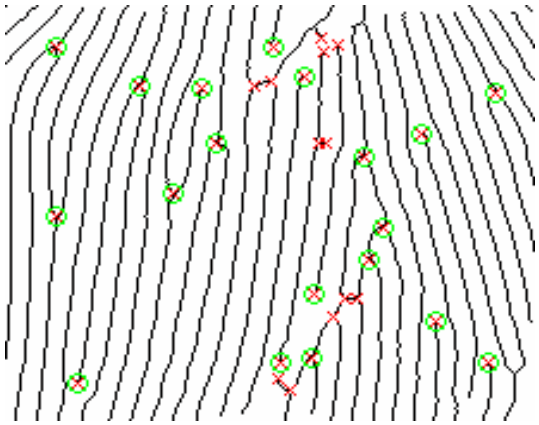
En este proyecto se ha implementado la técnica clásica de extracción de minucias, ya que permite detectar una adecuada cantidad de puntos característicos con unas sencillas reglas heurísticas, y además, con un tiempo de ejecución inmejorable.

3.5 Validación de las minucias

Sin embargo, el número de minucias candidatas detectadas con el algoritmo anterior es mucho mayor que el de las verdaderas, y por lo tanto,



a). Imagen original pre-procesada.



b). Imagen binarizada y esqueletizada, con las minucias identificadas.

Figura 3. Imagen de la huella tras dos etapas de procesado

muchas de las minucias detectadas y extraídas son falsas minucias, que requiere algoritmo de post-procesado para ser eliminadas.

En nuestro sistema se ha elegido un método de validación de minucias complejo pero de bajo coste computacional [9]. El algoritmo analiza la vecindad (de tamaño L=WxW) de cada minucia extraída en la etapa anterior (minucia potencial o candidata), y decide si se trata o no de una falsa minucia basándose en unas condiciones de contorno. Los resultados obtenidos en las pruebas revelan que, este método y junto con un simple tratamiento de las falsas minucias del margen de la imagen, valida una gran cantidad de minucias genuinas y elimina de modo satisfactorio, una gran cantidad de falsas minucias encontradas en las imágenes binarizadas y esqueletizadas.

3.6 Clasificación de las huellas

Una vez obtenida las minucias genuinas, se forman las plantillas, que son vectores con la información del tipo, posición y ángulo de orientación de cada minucia extraída de la imagen. Cuando el sistema entra en funcionamiento, se adquieren nuevas imágenes que, tras pasar por el proceso descrito de procesado digital de imagen, generan plantillas a verificar, esto es, determinar si la plantilla de entrada pertenece a la identidad reclamada.

Y esta tarea se encarga al clasificador. No obstante, a la hora de realizar esta tarea siempre se debe tener presente los siguientes efectos entre imágenes de un mismo individuo:

1. Hay traslaciones, rotaciones y deformaciones no lineales de las imágenes.
2. Aparecen falsas minucias, mientras que otras verídicas desaparecen.
3. No existe un comparador que entregue una coincidencia exacta entre dos vectores del mismo individuo, por tanto, es preciso establecer un margen de tolerancia entorno a cada minucia en el momento de realizar la comparación [10].

Para aliviar los efectos anteriores, se ha utilizado un clasificador de plantillas por semejanza basado en la transformada de Hough. Este método estima el valor de la rotación y traslación óptima entre dos plantillas, de tal forma que dichos valores son los que proporcionan el mayor grado de semejanza entre ambos vectores. Si dicha similitud es mayor que un umbral (calculado previamente en el proceso de entrenamiento del sistema, en el cual se establece el valor óptimo de decisión para cada individuo del sistema), se puede considerar que ambas huellas pertenecen a la misma persona.

4. Conclusiones

En el presente proyecto, se llevó a cabo el desarrollo de un sistema de autenticación de personas a través de la huella de la región dígito palmar. A pesar de trabajar con imágenes de huellas de baja calidad, se ha obtenido buenos resultados. Las pruebas de tests se hicieron sobre una base de datos de 532 imágenes de huellas, correspondiente a 38 usuarios, lo que significa 14 imágenes por persona; entre los usuarios seleccionados, 15 presentan unas huellas muy desgastadas, esta elección se debe exclusivamente, al interés por el estudio del comportamiento y el rendimiento del sistema bajo estas circunstancias.

Un sistema de autenticación de huellas ideal es aquel, que realiza un reconocimiento perfecto sobre la imagen de la huella original, sin ningún tipo de tratamiento de mejora. Desafortunadamente, los resultados obtenidos con las imágenes originales son pésimos, lo que surge la necesitad de un tratamiento de mejora antes de su procesado.

Existen numerosas técnicas de mejora de una imagen digital, y aquí se ha seleccionada una basada en la transformada de Fourier. Esta técnica presenta varias ventajas con respecto a las otras, por ejemplo, es particularmente adecuada para imágenes con poca contraste, por otro lado, tiene un coste computacional muy bajo; y lo más importante, es capaz de eliminar huecos y rupturas en la estructura de las colinas, dando un aspecto más continuo, recto y claro.

Después de aplicar la mejora, es preciso hallar la imagen binarizada y esqueletizada, antes de extraer las minucias. Para extraer las minucias, se requieren dos pasos. El primero, utilizando la técnica del número de cruce, se recorre la imagen buscando todas las terminaciones y bifurcaciones. Y el segundo, consiste en validar las minucias extraídas, es decir, se comprueba si dichos puntos cumplen ciertas condiciones. Los puntos singulares que logran superar con éxitos los dos pasos, son almacenados en vectores para su posterior clasificación.

Hay muchos tipos de clasificadores, y a priori, ninguno se puede considerar como el óptimo, ya que depende de la aplicación en donde se emplean. Por lo tanto, los criterios de selección dependerán del tiempo de cómputo, memoria requerida para almacenamiento, cantidad de información necesaria para la fase de entrenamiento, el tipo de aplicación en particular… en este caso, la elección fue un clasificador por plantillas.

Finalmente, los resultados obtenidos, tras una exhaustiva fase de verificación sobre la base de datos, revelan que el sistema presenta buenos rendimientos: con una tasa de acierto del 98,313%, y además, es capaz de autenticar a cualquier persona previamente registrada, en poco tiempo: menos de 2 segundos, e incluso, cuando la huella de ésta está muy desgastada; los cuales indican que este sistema satisface plenamente los objetivos marcados al comienzo de proyecto.

Bibliografías

[1] B. Millar, “Vital Signs of Identity”, *IEEE Spectrum*, vol. 31, no.2, pp. 22-30, 1994.

[2] L. Hong, A. Jain, “Integrating Faces and Fingerprints for Personal Identification”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no.12, pp.1295-1307, 1998.

[3] M. Eleccion, "Automatic Fingerprint Identification", *IEEE Spectrum*, vol. 10, pp. 36-45, 1973.

[4] B.Sherlock, D.Monro, K.Millard, "Fingerprint enhancement by direccional fourier filtering", *IEE Proc, Vision Image Signal Process*, vol.141, no.2, pp. 87-94, 1994.

[5] A.J. Willis and L. Myers, "A cost-effective fingerprint recognition system for use with low-quality prints and damage fingertips", *Pattern recognition*, vol.34, no2, pp.255-270, February 2001.

[6] Charles R. Gardina and Edward R. Dougherty, "Morphological Methods in Image and Signal Processing", *Prentice-Hall international editions*, 1988.

[7] Y. Y. Zhang, and P. S. P. Wang, "Analysis of thinning algorithms", *11th IAPR International Conference on Speech and Signal Analysis*, vol. 3, pp. 763-766, Sept. 1992.

[8] A. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-313, Apr. 1997.

[9] M. Tico and P. Kuosmanen, "An algorithm for fingerprint image postprocessing", *Conference Record of the Thirty-Fourth Asilomar Conference*, vol. 2, no. 29, pp. 1735-1739, Nov. 2000.

[10] N. Ratha, K. Karu, S. Chen and A. Jain, "A Real-Time Matching System for Large Fingerprint Databases", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol.18, no. 8, pp. 799-813, 1996.

Un novedoso indicador biométrico

La mano es una fuente de numerosos indicadores biométricos. Hasta la fecha se han desarrollado varias líneas de investigación entorno a las características peculiares de la mano, por ejemplo, las huellas dactilares, el contorno de la mano y las líneas o pliegues en la palma de la mano… a pesar de que cada uno de ellos necesitan diferentes y sofisticados algoritmos de procesados para extraer las informaciones contenidas en ella, todos ellos han obtenidos unos resultados bastante aceptables en el proceso de la identificación de la persona.

La región dígito palmar, por definición, es la región de la palma de la mano comprendido entre los pliegues de flexión (de la base de los dedos) y el pliegue inferior (comúnmente conocido como la línea del corazón). En esta zona, al igual que en la yema de los dedos, presenta unas estructuras singulares en forma de líneas en paralelo (colinas y valles), formando así las huellas palmares. Sin embargo, estas líneas se cruzan y a veces terminan en forma abrupta, estos puntos característicos que terminan o se bifurcan se conocen técnicamente como minucias.

Los sistemas de autenticación de personas basados en las huellas de la mano, trabajan precisamente con estos puntos características. Generalmente, mediante una serie de algoritmos de tratamiento de imágenes digitales, éstos mejoran la calidad de la imagen, para así, facilitar las tareas de las etapas siguientes:

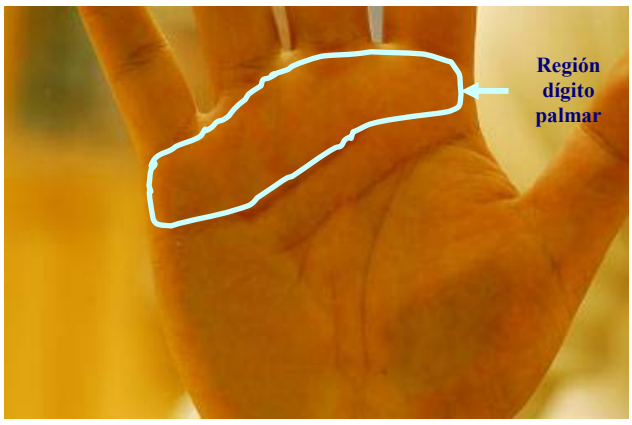


Figura 4. Ubicación de la región dígito palmar en la mano

binarización, adelgazamiento y extracción de minucias; y finalmente, mediante técnicas de clasificación se busca el grado de semejanza entre las minucias extraídas de una imagen, con las disponibles en la base de datos del mismo individuo para establecer la veracidad de la identidad de la persona.

En la práctica, la totalidad de la documentación consultada para realizar este proyecto está dedicada a sistemas de reconocimientos basados en las huellas dactilares, debido a la carencia absoluta de estudios e investigaciones en esta parte de la palma de la mano; no obstante, dada la similitud que hay entre éstas últimas y las huellas palmar (ambos presentan el mismo patrón, es decir, líneas en paralelo formando colinas y valles), entonces se entiende que es factible aprovechar las técnicas existentes para procesar las huellas dactilares, y extrapolar al procesamiento de las huellas de la región digito palmar.

Sin embargo, a pesar de lo apuntado en el párrafo anterior, han sido necesarios desarrollar nuevos algoritmos o adaptar los algoritmos desarrollados con las huellas digitales para este sistema, ya que la región dígito palmar presenta unas peculiaridades que no se ven en la yema de los dedos.

En efecto, una de las mayores diferencias que existe entre una huella digital y palmar es el estado de desgaste de la piel de ésta ultima. Si bien las yemas de los dedos no sufren excesivamente de erosiones y rozamientos, pues la palma de la mano de cada individuo está en continuo fricción con los objetos que entran en contacto. Y lo anterior se traduce a menudo en pieles lisas, pulidas, y con muy poca relieve o contraste de la huella (o que es lo mismo, colinas y valles), que consecuentemente, dificultará en los sistemas de autenticación, ya que éstos se basan su reconocimiento precisamente en estos patrones de la piel.

Además, en la piel de las personas de mayor edad es propenso a las apariciones de arrugas, y éstas interfieren de modo aleatorio en las ordenadas líneas de colinas y valles,

a). Huella digital

b). Huella palmar

Figura 5. Diferencia entre una huella digital y una huella palmar

deteriorándose así la definición del patrón; si a esto último, se le suma una palma lisa, pulida incluso, callos,… y se tendrán lugar unos factores condicionantes de la aparición de falsos patrones o falsas minucias, y que a su vez, son los responsables de que el sistema falla o que baje su rendimiento.

Como consecuencia de lo anterior, los algoritmos de este sistema debe ser capaces de subsanar estas interrupciones, e incluso unir las colinas si es preciso, para darle un aspecto más continuo y compacto. No hay más que decir que, en las técnicas basados en huellas digitales, no tienen que preocupar en exceso por este punto, y por lo consiguiente, la aplicación directa de éstas en este sistema producirán unos resultados muy ineficientes.

Resultados

Para obtener unos resultados concluyentes del sistema desarrollado, se ha procurado confeccionar una base de datos que está estadísticamente bien balanceada en cuanto a sexo y edad (entre los 18 y 70 años) de los individuos seleccionados; también se ha tenido en cuenta la calidad de sus huellas, que básicamente se pueden distinguir en tres categorías: alta, media y baja calidad. Por huella de baja calidad nos referimos a huellas sin patrón visible, esto es, que presentan un aspecto liso y pulido.

Con las imágenes adquiridas en la base de datos inicial, 14 por persona, se ha utilizado 5 para entrenar el sistema y 9 para verificar el sistema. Con las 5 imágenes de entrenamiento de cada usuario se han determinado sus plantillas y los umbrales a partir del cual se considera aceptada la identidad reclamada.

Así, se han realizado 4332 pruebas en la fase de verificación del sistema. Estas pruebas indican que el índice de fiabilidad o número de aciertos se sitúa en 98,33%. Cabe resaltar que este sistema presenta un resultado global bastante bueno, e incluso, muy superiores a otros sistemas de autenticación basados en otros indicadores biométricos estudiados previamente. Evidentemente, para ser el resultado obtenido en un sistema prototipo, que ya se puede considerarse bastante óptimo, entendemos que es factible mejorarlo, aún más, en una versión optimizada.

Dada la diversidad (edad, sexo, calidad de las huellas…) de las imágenes de la base de datos, también se han realizado estudios en función del nivel de calidad de las huellas de la región dígito palmar, observando que si bien el sistema presentan un clara dependencia de la calidad de la huella, éste presenta una buena tolerancia con respecto a este factor, es decir, trabajando exclusivamente con imágenes de huellas de alta calidad, se obtiene en nuestra base de datos una fiabilidad del 100%; y si por el contrario se trabaja solamente con imágenes de baja calidad, el rendimiento decae levemente hasta 96,34 %.

De todos modos, se puede considerar bastante exitosos los resultados mostrados en este análisis, dada la cantidad de imágenes de baja calidad incluida en la base de datos. De hecho, en las publicaciones consultadas acerca de los sistemas de autenticación (la mayoría de los cuales ni siquiera trabajan con huellas de baja calidad), muestran unos resultados mucho más pesimistas, lo cual es un indicativo de que éste sistema funciona incluso mejor que otros del mercado actual bajo unas condiciones mucho peores.

Por otro lado, el estudio de los resultados por edades revela que el grupo de personas con el que se han obtenido peores resultados es el de mayor edad (96,14%). Esto se puede explicar debido al número de arrugas de la piel de éstos últimos, que se traducen en una gran cantidad de falsas minucias, lo cual afecta negativamente al funcionamiento del sistema.

Finalmente, hay otro aspecto importante a analizar: el tiempo de ejecución del sistema en funcionamiento. Debido a que se ha desarrollado un sistema con orientación para aplicaciones de tiempo real, este factor se convierte en un elemento crucial en la viabilidad del sistema. Muchos sistemas actuales de autenticación de personas basadas en huellas, requieren bastante tiempo de ejecución, algunos rondan alrededor de los 20 segundos, y otros más rápidos, están en unos 4 segundos.

Tras realizar las evaluaciones pertinentes se ha logrado un tiempo de respuesta inferior a 2 segundos con el sistema programado en metalenguaje. Programar el sistema en otro lenguaje como el C conlleva una reducción de 5 a 6 veces el tiempo de ejecución. En este caso, no sólo se ha alcanzado este objetivo, sino también se ha superado con creces a los sistemas actuales, siendo uno de los más competitivos en este sentido.

Aplicación del proyecto

En el mercado actual, existen numerosos sistemas biométricos que basan su acción en el reconocimiento de diversas características. Cada una de las técnicas anteriores posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir qué técnicas utilizar para una aplicación específica. Por ejemplo, una huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales…

Debido a las diferencias señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades. Una compañía puede incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la autenticación [2], y los resultados alcanzados por el sistema conjunto son mejores que los obtenidos por separado. En efecto, las limitaciones de las alternativas por separado son soslayadas, logrando además respuestas exactas con un tiempo de proceso adecuado.

Por tanto, el sistema desarrollado en este proyecto fin de carrera se podría combinar, o bien, con otros sistemas de reconocimiento de personas basados en otros indicadores biométricos de la mano: geometría, huella dactilar, líneas de la palma de la mano… formando así un sistema que proporcionará un altísimo nivel de seguridad; o bien, constituirse por sí mismo como un sistema de autenticación, como es el caso de este prototipo.

Como ya se comentó anteriormente, este sistema posee tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella mediante un sensor. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos (una imagen, por ejemplo) con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema.

Pues bien, el mercado actual ofrece un amplio

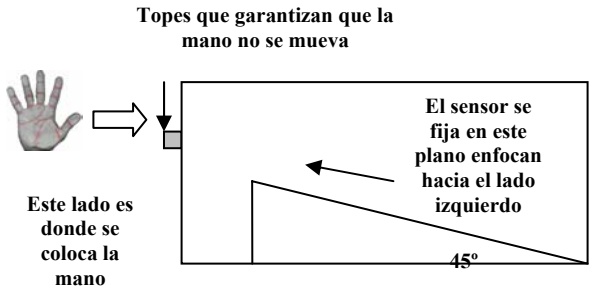


Figura 6. Perfil lateral del soporte

Figura 7. Imagen exterior e interior del soporte de la cámara.

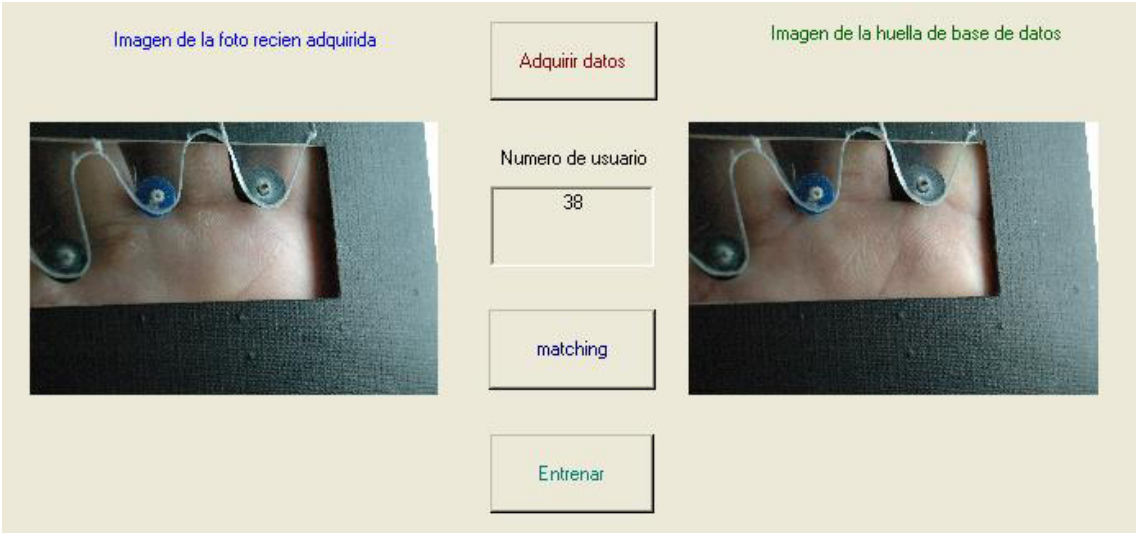


Figura 8. Interfaz del sistema desarrollado

abanico de posibilidades en cuanto al sensor se refiere, tales como escáner, lector láser, cámaras digitales… todos estos pueden utilizarse perfectamente en la mayoría de los sistemas de autenticación, aunque lo más común es encontrar con un tipo de sensor en concreto para determinados tipos de aplicaciones, y en el caso de este proyecto, se ha utilizado una cámara digital.

Tras experimentar con diferentes tipos de iluminación, ángulo, distancia de enfoque… se ha construido un soporte para la cámara, en el cual se ilumina la palma de la mano de forma oblicua con un fluorescente en el mismo plano que la mano, y con el foco de la cámara a 30 centímetros de la palma de la mano formando un ángulo de 45 grados. Una idea intuitiva de esta estructura se observan en las figuras anteriores.

Una vez que la cámara ha sido fijada en el soporte, se conecta a un PC (o cualquier otro sistema en donde se encuentran ubicados los algoritmos desarrollados) para confeccionar la base de datos, y posteriormente, mediante un sencillo interfaz con el usuario ya es posible poner el sistema en funcionamiento.

ANEXO

Publicaciones:

[1] Zai Jian Jia Li, Miguel Ángel Ferrer Ballester, Carlos M. Travieso and B. Alonso, "Biometric base on the ridges of the palm skin over the head of the second metacarpal bone". *Artículo aceptado por IEE Electronic letters, pendiente de publicación en 2006*. [Internacional]

[2] Zai Jian Jia Li, Miguel Ángel Ferrer Ballester, Jesús Bernardino Alonso Hernández, Carlos M. Travieso González y Fabio Román Arbelo, "Autenticación de personas a partir de la biometría de la región dígito palmar". *Artículo para Vector Plus de Fundación Universitaria de Las Palmas, pendiente de publicación en 2006*. [Nacional]