Análisis del proceso de reconocimiento de una huella dactilar

Analysis of the process of a fingerprint recognition

Francy Julieth Pineda Bohórquez*

Resumen

El reconocimiento de huellas dactilares es uno de los métodos más populares empleados con mayor éxito para la identificación de personas. Se busca obtener la imagen de una huella dactilar de alta calidad, y así poder observar con más detalle cada una de las características propias de la huella (minucias y patrones). Para esto, es necesario que las imágenes que se van a estudiar sean procesadas de forma rigurosa, usando un método específico para obtener la imagen apropiada que contenga una gran cantidad de información para lograr una identificación correcta.

En este documento se hace un análisis del proceso que se sigue para realizar el reconocimiento de una huella dactilar. Las temáticas se encuentran distribuidas de la siguiente forma: en el numeral 3 se exponen las características de las huellas dactilares; en el numeral 4, el proceso de obtención y reconocimiento de una huella dactilar; en el numeral 5 se menciona el hardware y las técnicas de reconocimiento empleadas. Y finalmente se explica un procedimiento de utilización probable para lograr cada uno de los numerales 3,4 y 5 de forma correcta.

Este artículo hace parte del estudio teórico y exploratorio, desarrollado en la línea de investigación en procesamiento de señales, como parte de las actividades de formación del semillero de investigación del grupo DSP-UPTC.

* Escuela de Ingeniería Electrónica. Grupo de Investigación en Procesamiento de Señales DSP, Universidad Pedagógica y Tecnológica de Colombia, Sogamoso. E-mail:Francypineda77@gmail.com

Palabras clave
Huella dactilar, seguridad biométrica, procesamiento digital de imágenes.

Abstract

The recognition of fingerprints is one of the most popular methods successfully used for identifying people. It seeks to obtain a high quality fingerprint image, to observe with more detail each of the characteristics (minutiae and patterns). For this, it is necessary that the images that are going t study are processed using a specific method to obtain the appropriate image that contains information to achieve the correct identification.
In this document we analyze the process to make fingerprint recognition. The themes are distributed in the following way: in section 3 are shown the fingerprints characteristics; in section 4, the process of obtaining and recognizing fingerprints; section 5 refers to the hardware and recognition techniques. And finally we explain the procedure of probable use to achieve each of the numerals 3, 4 and 5 correctly.
This article is part of theoretical and exploratory study, carried out in the research in signal processing, as part of training activities of DSP-UPTC research group.

Keywords
Fingerprint, biometric security, images digital processing.

Introducción

En la actualidad, la seguridad biométrica usa el reconocimiento de huellas dactilares, para lograr la identificación correcta de una persona y obtener determinado acceso sin temor a que este no corresponda al usuario. Emplear huellas dactilares para obtener una identificación es un método confiable de seguridad, puesto que las huellas dactilares son únicas para cada individuo.

El proceso de reconocimiento de una huella consiste en: primero obtener una imagen para guardarla en una base de datos (esta será la imagen que se va a comparar), luego la imagen de la huella que va a ser identificada se compara con las que están previamente almacenadas en dicha base de datos.

Para lograr el reconocimiento es necesario que la imagen tomada sea de alta calidad, así es posible la extracción de información de dicha huella por medio de un software que la convierte en un código binario. Este es el método más conveniente para la extracción de información de las huellas, para posteriormente lograr su comparación e identificación empleando el formato numérico (sistema binario).

I. Objetivos

- Comparar dos imágenes con el fin de conocer si corresponden a la misma persona.
- Reconocer a un usuario al ingresar su huella a una base de datos.
- Aplicar el proceso de reconocimiento de una huella dactilar para la seguridad de la identidad de una persona.

II. Características de las huellas dactilares

El reconocimiento de huellas dactilares se fundamenta en la biometría, la cual es una tecnología de seguridad basada en el reconocimiento de una característica física e intransferible de la persona. Dentro de las características más empleadas para aplicaciones de seguridad en empresas y hogares se encuentra la huella dactilar (página web de Homini, 2004).

Las huellas dactilares son una característica propia de la persona y se clasifican en cuatro tipos: espiral, arco, lazo y compuesta (González, 2004). Estas clasificaciones se pueden observar en la Figura 1.

Las huellas dactilares son diseños virtualmente únicos y están compuestas por valles y crestas de piel en la punta de los dedos. Los valles son cambios epidérmicos en las zonas de las plantas y las crestas son bifurcaciones que se forman por una combinación de factores genéticos y ambientales aleatorios; como lo son la posición del feto en un momento particular y la composición y densidad exacta del líquido amniótico que lo rodea (González, 2004).

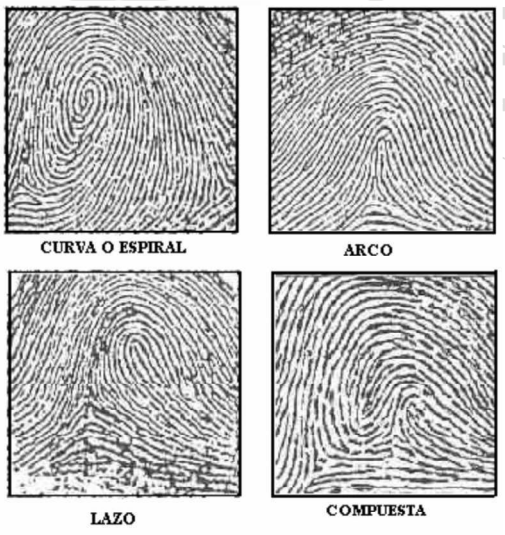

Fig. 1. Clasificación de huellas dactilares. Fuente: (Báez, 2003).

III. Proceso de obtención y reconocimiento de una huella dactilar

1) Obtención de la imagen de una huella dactilar

Para obtener la imagen apropiada de la huella dactilar de un usuario, es necesario un lector o escáner (lector óptico, lector capacitivo), a fin de lograr una imagen bien detallada, donde se puedan diferenciar los cambios de las minucias (Aguilar,Sánchez, Toscano, Nakano &Pérez, 2008). Para ello es necesario que en el momento del escaneo la huella se mantenga firme en un solo lugar, para evitar errores posibles en la imagen; también será útil que la superficie de la huella se encuentre limpia y seca. Es preciso tomar varias imágenes para así obtener más información de dicha huella, sin temor a contar con información superficial.

2) Selección de la imagen adecuada para comparar

Ya que se cuenta con varias imágenes de la huella del usuario, es necesario corregir su calidad utilizando filtros de Gabor (corrige imperfecciones de la imagen), los cuales son el método más confiable, pues logran una óptima resolución de la imagen; también es preciso adelgazar la imagen, es decir, aplicar un algoritmo que entrega como resultado una imagen con bordes de un píxel de grosor, el resultado de este procedimiento se observa en la Fig. 2. En el momento de guardar la imagen en la base de datos, esta será recortada en sus extremos para recopilar la información de la parte central de la huella (Aguilar et al., año).De la obtención de esta imagen depende todo el estudio, por lo tanto es muy importante que no se cometan errores en este procedimiento.

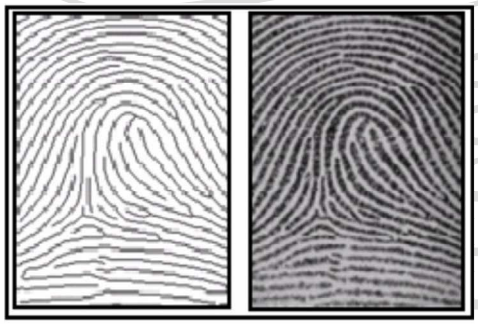

Fig 2. Huella adelgazada. Fuente: (Báez, 2003).

1) La imagen es escrita en forma binaria

Como ya se cuenta con la imagen adelgazada, que se explicó en la sección *B,* es posible extraer las minucias de la huella dactilar que constituyen el patrón biométrico de la huella.

El proceso para obtener la imagen de forma binaria consiste en llevarla de escala de grises, (normalmente 256 bits de intensidad) a una imagen blanco y negro, (2bits de intensidad) (Báez, 2003).

Después de obtener la imagen en blanco y negro, se realiza el proceso de binarización que consiste en la clasificación de los pixeles en cresta/no-cresta, es decir, en 1 y 0.Una vez leída toda la imagen se obtendrán los puntos característicos con sus coordenadas relativas en la imagen, como se aprecia en la Figura 3.

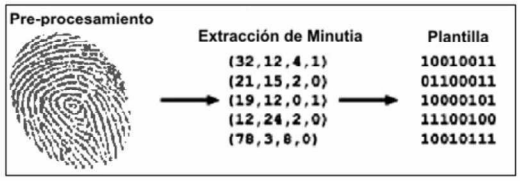

Fig.3. Pre-procesamiento de la huella. Fuente: (Página web Tecmex, s.f.).

3) Reconocimiento de la huella

El reconocimiento se hará empleando tres importantes características de la información extraída de las huellas: coordenadas, distancia y ángulos.

El proceso se adelanta de la siguiente forma: la imagen de entrada se convierte en una matriz de 4x500, y esta matriz es comparada con cada una de las almacenadas en nuestra base de datos. Primero se localizan los vectores con distancias iguales y se toman únicamente los que tienen el mismo ángulo, después se descartan los vectores que tienen coordenadas muy diferentes y de esta forma se asegura el reconocimiento de la huella dactilar (Aguilar et al., 2008)

Para esto se utilizan algoritmos de complejo desarrollo, técnicas de inteligencia artificial y características de las impresiones digitales (Carrión & Barragán, s.f.). De esta forma llegamos a identificar si la huella ingresada corresponde con la que el usuario ingresó en la base de datos inicialmente.

IV. Hardwarey técnicas de reconocimiento

1) Hardware

Una variedad de tipos de sensores ópticos, capacitivos y térmicos, son utilizados para tomar información de imágenes digitales de la superficie de una huella dactilar.

Los sensores ópticos toman una imagen de la huella, y son el tipo de sensor más

usado hoy en día. Estos toman una imagen de la huella y generan una imagen de las crestas y valles que conforman la huella digital. Funcionan con un dispositivo CCD (Charged Coupled Device), que produce una señal eléctrica en respuesta a fotones de luz. Cada diodo graba un píxel; es decir, un pequeño punto que representa la luz que le es reflejada.

Los sensores capacitivos determinan el calor de cada píxel basándose en la capacitividad medida. Los escáneres térmicos requieren el contacto de un dedo a través de una superficie para medir la diferencia de temperatura en un tiempo dado, a fin de crear una imagen digital (Página web datasecurity, 2006).

2) Técnicas de reconocimiento

Las dos categorías principales de las técnicas de coincidencia de huellas dactilares están basadas en minucias o por patrones. La coincidencia por patrones simplemente compara dos imágenes para ver cuán similares son. Esta técnica es utilizada en sistemas de huellas dactilares para detectar duplicados.

La técnica de reconocimiento más utilizada, es la basada en minucias, específicamente en la ubicación y la dirección de cada punto, teniendo en cuenta estas minucias se remite a la base de datos que contiene huellas digitales ingresadas previamente, las cuales son comparadas con la imagen tomada. Si se encuentra semejanza entre la imagen tomada y la almacenada en la base de datos, el software biométrico permitirá el acceso al sistema, de otro modo será rechazado (Página web datasecurity, 2006).

V. Proceso completo para el reconocimiento de una huella dactilar

Para comenzar, es necesario contar con las dos imágenes que se van a comparar; la que está almacenada en una base de datos para la identificación del usuario, la siguiente imagen es la que se ingresa con el lector (este se elige según el grado de seguridad que se busque); una vez se disponga de estas dos imágenes, se usa el software MATLAB, que tiene la capacidad de hacer todo el proceso para reconocer la imagen.

Es importante que se entienda que cada uno de los siguientes procedimientos hechos en MATLAB se logra con funciones ya existentes diseñadas especialmente para este tipo de aplicación.

Se inicia con la lectura de la imagen en MATLAB, luego se visualiza y se modifica a escala de grises, con el fin de contar con su histograma que nos dice qué tantos bits de determinada intensidad existen en la imagen, luego se pasa la imagen a blanco y negro. Al tener la imagen de esta forma será más fácil comparar de forma binaria (matricial) la imagen, para posteriormente aplicar un programa que se encargará de comparar la imagen ya almacenada con la que se acaba de transformar, y lograr así una identificación correcta del usuario.

VI. Conclusiones

Utilizar huellas dactilares en seguridad biométrica es un método confiable para la identificación de personas, ya que este rasgo en particular es único en cada ser humano. Esta característica permite que las huellas sean comúnmente empleadas en diversos sistemas de seguridad, logrando así que estos sean más confiables y seguros.

Para obtener el reconocimiento de una huella dactilar, es necesario tener en cuenta toda la secuencia numérica, es decir, la forma binaria que la representa, pues es de esta manera que se obtienen rasgos propios, y el proceso de reconocimiento se hará en forma detallada, así se obtiene la identificación correspondiente a la cual pertenece dicha huella.

Para obtener un resultado óptimo en el momento de identificación de la huella dactilar, es importante el tipo de lector que se elija para obtener así la imagen apropiada, puesto que de ella depende todo el proceso de reconocimiento.

Lista de referencias

Aguilar, G., Sánchez, G., Toscano, K., Nakano, M. &Pérez, H (2008). *Reconocimiento de huellas dactilares usando características locales.* 2008,Medellín, Colombia,Universidad de Antioquia,*Facultad de Ingeniería Universidad de Antioquia,* Núm. 46, pp.101-109

Báez, L. (2003). *Extracción de características de Galton de huellas dactilares por procesamiento digital de la imagen*. Recuperado dehttp://www.luchonet.com.ar/huellas/trabajofinal/Car%C3%A1tula-para-utnfrc.pdf

Carrión, C. &Barragán, D.(s.f.). Recuperado de http://www.scribd.com/doc/20775630/Huellas-dactilares

Cómo funcionan los lectores de huellas dactilares. (s.f.).Recuperado dehttp://www.tecmex.com.mx/promos/bit/bit0903-bio.htm

González, M.(2004). *Introducción ala dactiloscopia como método de identificación*. Recuperado de http//cienciaforense.com/pages/evidenciafisica/dactiloscopia.htm

Plataforma biométrica Homini. (2004). Recuperado de http: //www.homini.com/new_page_5.htm

Reconocimiento de huellas dactilares.Comité de Seguridad Nacional de los Estados Unidos.(Agosto, 2006). Recuperado dehttp://www.datasecuritys.com/docs/FPRecover.pdf