

Tecnologías de identificación por huella dactilar¹

Dr. Gerik Alexander v.Graevenitz

Applied Biometrics GmbH, Bonn, Germany

10 de Diciembre de 2007

Biometría. Resumen.

La Biometría se define como la identificación automatizada de una persona viva, basada en las características fisiológicas o de comportamiento. Hay muchos tipos de tecnologías biométricas en el mercado que procesan las siguientes variables biométricas: reconocimiento de rostro, huellas dactilares, geometría manual, sistema venoso de la retina, iris y reconocimiento de firma y voz.

Los métodos de identificación biométrica se prefieren a los métodos clásicos de identificación por varias razones:

- Es necesaria la presencia física del individuo que va a ser identificado.
- Con la identificación basada en técnicas biométricas no es necesario recordar una contraseña o llevar una tarjeta de identificación.

La revolución en la tecnología de la información ha producido un rápido incremento en el uso de PINS y contraseñas. Por esto es necesario restringir el acceso a datos personales. Las técnicas biométricas, que sustituyen el uso de PINS y contraseñas, son más prácticas para el usuario y pueden prevenir con mucha más efectividad el acceso sin autorización o uso fraudulento de ATMs, Time & Attendance Systems, teléfonos móviles, ordenadores, sistemas y redes informáticas, tarjetas de identificación, etc. Contraseñas y PINS se pueden olvidar; métodos de identificación basados en tarjetas como pasaportes, carnet de conducir o de seguro de sanidad pueden también olvidarse, extraviarse, o perderse.

En la actualidad se utilizan varios tipos de sistemas biométricos para la identificación en tiempo real. Los más populares son la geometría facial y huella digital. Pero existen otros como por ejemplo: la geometría manual, el sistema venoso de la retina e iris, la voz y la firma

Tecnologías de identificación por huella dactilar

La identificación basada en la huella dactilar es uno de los métodos más antiguos de identificación biométrica. Su historia se remonta al año 2200 a.C. El uso de huellas dactilares como código personal tiene una larga tradición y ya era utilizado por los sirios, babilonios, chinos y japoneses. La dactiloscopia (sinónimo de identificación de

¹ Publicado en A&S International con el título "Sensing Fingerprints", Volume 52, Taipei, 2003, páginas 102-104

huellas dactilares no basada en ordenador) se usa en la investigación criminal desde 1897. La huella dactilar consta de crestas papilares (las líneas que cruzan en sentido ascendente la yema de los dedos) y surcos (los espacios entre las crestas). La combinación de crestas y surcos es única en cada individuo.

La identificación por huella dactilar se puede dividir en dos grandes grupos:

- Específica- basada en los puntos de discontinuidad de terminaciones y bifurcaciones, denominados puntos de minucia.
- General- aproximación macroscópica. Se tienen en consideración el sentido de las crestas papilares, por ejemplo arcos, curvas y espirales.

Podemos decir que la identificación dactilar es muy precisa ya que el índice de error es muy bajo. El precio de estos sistemas comparados con otros sistemas biométricos es muy bajo y su aceptación por el usuario muy alta. La base del éxito de este sistema es su aplicación en diferentes campos. Es una tecnología comprobada y su capacidad de registrar la diversidad de huellas aumenta su exactitud y flexibilidad drásticamente.

Sensores Ópticos

El método óptico es uno de los más comunes. El núcleo del escáner óptico es una cámara CCD (Dispositivo de Carga Acoplada)

La cámara CCD consiste simplemente en una serie de diodos sensibles a la luz llamados fotolitos. Normalmente el dedo se coloca en una placa de cristal y la cámara hace una foto.

El sistema CCD tiene una capa de LEDs (diodos emisores de luz) para iluminar las crestas y surcos del dedo. La ventaja de los sistemas ópticos es su bajo precio; la desventaja es que son bastante fáciles de falsificar. Otro problema es que en ocasiones pueden permanecer en la superficie del sensor algunos rasgos del dactilograma anterior.

Empresas líderes en la producción de este escáner son: Delsy, Dermalog, Smiths Heimann Biometrics (subempresa de Jenoptik/Rheinmetall)

Sensores Termoeléctricos

El método termoeléctrico es menos común. Actualmente sólo existe en el mercado el Atmel Fingerchip™.

El Fingerchip™ utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas (*slices*) y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite al Fingerchip™ obtener una gran cualidad, 500 puntos por imagen impresa de la huella dactilar con 256 escalas de gris.

El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran calidad incluso cuando las huella dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua.

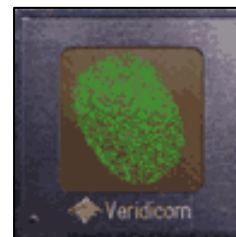
Además, también cuenta con la ventaja de autolimpieza del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que permite que se copie la huella para falsificarla y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el Fingerchip esté por encima de otras tecnologías. El Fingerchip™ funciona con bajas temperaturas, alto porcentaje de humedad, etc.

Otra ventaja es la reproducción de una imagen grande de alta calidad y siempre un sensor limpio. La desventaja es que la calidad de la imagen depende un poco de la habilidad del usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente. Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar.

El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona.

Sensores Capacitivos

El método capacitivo es uno de los más populares. Al igual que otros escáner, genera una imagen de la cresta y los valles. En la superficie de un circuito integrado de silicón se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato.



Veridicom 5th sense™

La mayor ventaja es que se requiere una huella real pero se pueden presentar problemas si la yema del dedo está húmeda o muy seca. En este caso se obtendrán imágenes negras o pálidas.

Entre las empresas líderes en este sector se encuentran: Infineon, Veridicom, Sony y ST Microelectronics.



Infineon FingerTIP™

Sensores E-Field (de Campo Eléctrico)

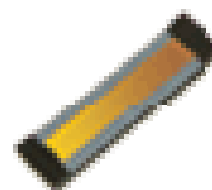
El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, del “mundo real”, como por ejemplo piel húmeda, seca o dañada.



Authentec AES4000

Esta tecnología origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador *under-pixel* para medir la señal. Los sensores reproducen una imagen clara que se corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podrían.

En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma.



Authentec AES2500

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la

superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de campo eléctrico.

Desde hace poco existe también un sensor más fuerte basado en esta tecnología que saldrá al mercado en pocos meses.

Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

Sensores sin contacto

Un sensor sin contacto funciona de forma similar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Una desventaja a tener en cuenta es que a través de este hueco pueden llegar polvo y suciedad hasta el cristal óptico con la correspondiente distorsión de la imagen. Otro punto es que las huellas escaneadas son esféricas lo que origina un complejo algorítmico mucho más complejo.

Surface Pressure Sensor

The principle of pressure sensing is that when a finger is placed over the sensor area, only the ridges of the fingerprint come in contact with the sensor piezo array. The valleys in contrast have no contact with the sensor cells. A main difference for the further recognition and matching to other sensors we have is pressure sensors generate a 1-bit binary image. A 1-bit image has less information than an 8-bit gray-scale image.

A surface pressure sensor can be considered as allowing clearly to sense both dry and wet fingers. Furthermore it has a large sensing area, which enables it to capture a complete fingerprint for better accuracy of recognition that leads to a lower EER (Equal Error Rate.)



BMF BLP100-Sensor

Identificación de la huella dactilar

La identificación basada en la huella dactilar se puede dividir en dos grandes grupos: específica (basada en los puntos de minucia) y general (analiza la estructura global). La identificación automática de huellas dactilares se hace casi siempre basándose en los puntos de minucia. Se denomina así a las características específicas de las yemas de los dedos que pueden presentar como bifurcación o final de cresta.



Terminación dactilar



Bifurcación dactilar

La individualidad de la huella dactilar se determina por las crestas y surcos que la componen. Una huella dactilar completa consta con un promedio de 100 puntos de minucia. El área que se mide consta con un promedio de 30 a 60 puntos de minucia dependiendo del dedo y el sensor.

Los puntos de minucia se representan por una línea de puntos en un sistema de coordenadas. Estos se añaden con el ángulo de la tangente del punto de minucia local a un código dactilar o directamente a una plantilla de referencia. La plantilla puede constar de más de un código dactilar para ampliar la cantidad de información así como el área a considerar. En general esto lleva a una calidad de plantilla más alta y por tanto a un valor también elevado de similitud entre plantilla y modelo.

El tamaño de plantilla varía entre 100 bytes y 1500 bytes, dependiendo del algoritmo y la calidad de la huella. Sin embargo, muy pocas veces se dan huellas sin ningún tipo de punto de minucia. Esto produce un índice de error registrado (FER). Resulta también muy difícil extraer los puntos de minucia cuando la huella dactilar es de baja calidad.

Conclusión

Eligir una tecnología biométrica, en especial un sensor de huellas dactilares, parece ser muy difícil. Cada método de sensores tiene sus ventajas y desventajas. Por consiguiente no es posible hacer una recomendación general para cada tecnología especial. Esto demuestra que elegir un sensor de huellas dactilares depende de la aplicación a la que el cliente quiera ser implementado / añadido. Esto depende estrictamente del entorno. La combinación de los algoritmos y los sensores de huellas dactilares es muy importante en relación al índice de error alto (EER).