UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

ESPECIALIZACIÓN EN COMUNICACIONES Y
REDES DE COMUNICACIÓN DE DATOS

ESTUDIO DE TÉCNICAS BIOMÉTRICAS PARA VERIFICACIÓN DE IDENTIDAD EN SISTEMAS DE CONTROL DE ACCESO

Autor: Lic. Marta Rodríguez Martínez *Tutor: M.Sc. Vincenzo Mendillo*

Caracas, Enero de 2004

UNIVERSIDAD CENTRAL DE VENEZUELA
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA ELÉCTRICA

ESPECIALIZACIÓN EN COMUNICACIONES Y
REDES DE COMUNICACIÓN DE DATOS

Estudio de Técnicas Biométricas para Verificación de Identidad en Sistemas de Control de Acceso

Trabajo Especial de Grado presentado como requisito para optar al Titulo de Especialista en Comunicaciones y Redes de Comunicaciones de Datos

Elaborado por: Lic. Marta Rodríguez Martínez

Visto Bueno

Tutor: M.Sc. Vincenzo Mendillo

Caracas, Enero de 2004

DEDICATORIA

A Francisco, la persona que más amo en mi vida, por compartir todos los momentos difíciles y exitosos de toda mi carrera y darme el animo necesario para continuar y culminar este gran reto.

A mi querida mamá y papá: Maria Marta y Nemesio, gracias a ellos soy la persona que soy hoy en día.

A mi hermano Víctor, quien estuvo siempre apoyándome incondicionalmente.

Y a Dios Todopoderoso y La Virgen Milagrosa por estar siempre acompañándome.

AGRADECIMIENTOS

Al Profesor Vincenzo Mendillo, mi tutor, por su orientación, dedicación, paciencia, comprensión y amistad, siendo participe de mi formación académica y profesional, durante todo este tiempo, permitiéndome culminar esta meta en mi vida.

A mis compañeros de estudios con los cuales compartí grandes momentos de mi carrera.

A mi amigo Raúl que me ayudo muchísimo con sus conocimientos.

A mi amiga Angélica porque siempre me apoya en todas mis decisiones.

A todos aquellos que de una manera u otra estuvieron conmigo en este gran recorrido.

A todos muchísimas gracias…

RESUMEN

Una de las amenazas más peligrosas para la seguridad es la suplantación, en la cual alguien se hace pasar por otra persona. Los sistemas de seguridad enfrentan esta amenaza mediante el reconocimiento y la autenticación. El reconocimiento es el mecanismo mediante el cual se identifica a un individuo especifico entre muchos, mientras que la autentificación se ocupa de verificar la identidad de ese individuo. El sistema de reconocimiento y autenticación del usuario se puede clasificar en base a lo que él sabe (una contraseña), en base a lo que él posee (una tarjeta inteligente) o en base a sus características humanas (biométricas).

En este estudio se examinan las dos categorías de las técnicas biométricas. La primera basada en las características fisiológicas de una persona y que incluyen: verificación de la huella dactilar, análisis del iris, análisis facial, geometría de la mano o patrones de vena de la mano, reconocimiento de la forma del oído, detección del olor, análisis del patrón del ADN y análisis de los poros sudoríficos. La segunda mide el comportamiento de una persona, e incluyen verificación de la firma manuscrita, análisis del tecleado y análisis de la voz, entre otros.

Hay dos preocupaciones básicas en estas tecnologías: la tolerancia al error y el almacenaje de las plantillas, las cuales son datos almacenados que se derivan de las características biométricas de un individuo. El ajuste de la tolerancia del error de estos sistemas es crítico para su funcionamiento. Los dos tipos de error (falso rechazo y falsa aceptación) deben ser bajos y estar muy bien especificados por el fabricante del equipo. Las plantillas pueden ser almacenadas en varios lugares dependiendo del uso y los requisitos de seguridad del sistema. Las plantillas se pueden almacenar en el dispositivo biométrico, en una base de datos central, en tarjetas magnéticas o inteligentes.

Por otra parte la confiabilidad y la aceptación de un sistema de seguridad dependen de cómo el sistema se comporta ante amenazas y su eficacia para identificar los abusos al sistema. Hay varios tipos de amenazas a las que las tecnologías biométricas se ven expuestas y estas amenazas puede caer en una de las estas tres categorías principales: físicas, humanas y técnicas.

Basados en la literatura, se muestran en este estudio los criterios para evaluar los métodos y dispositivos biométricos. El primer grupo de criterios es para evaluar los protocolos, los algoritmos y los códigos usados en los sistemas biométricos. El segundo grupo es utilizado para evaluar aspectos operacionales, técnicos, de costo y de fabricación de estos sistemas.

Como todas las tecnologías de seguridad existentes, la biometría no es invulnerable, tal como lo demostró el criptógrafo japonés Matsumoto que mediante un sistema basado en huellas artificiales de gelatina pudo engañar a 11 tipos de sensores biométricos.

En el presente estudio, se logró vulnerar un sistema de escaneo óptico (mouse biométrico) basado en el reconocimiento a través de la huella dactilar, sin mayores recursos e inspirados en el experimento de Matsumoto utilizando para ello solo plastilina común para la elaboración de los moldes y materiales como gelatina y silicona para la fabricación de las distintas huellas artificiales, logrando que el lector óptico del mouse reconociera como validas dichas huellas.

En conclusión, todas las tecnologías biométricas tienen sus puntos fuertes y sus puntos débiles, se trata de elegir la que para el entorno en particular, sus ventajas superen a sus inconvenientes.

ÍNDICE

CAPITULO I

EL PROBLEMA Y LOS OBJETIVOS DE LA INVESTIGACIÓN

1.1 Planteamiento del problema

La identificación correcta de individuos ha sido siempre un problema de capital importancia en el ámbito de las tecnologías de la información y es por ello que hoy día se cuenta con diversas tecnologías para identificar a individuos al momento que ingresan a instalaciones, recintos o al utilizar dispositivos informáticos, por ejemplo computadoras y cajeros automáticos. Una de esas tecnologías es la biometría, cuya función es la identificación correcta del individuo a partir de las características que le son propias, por ejemplo la voz, cara, iris, huella dactilar, forma de la mano y firma manuscrita.

El desarrollo de la sociedad de la información, con el aumento incesante de las comunicaciones, tanto en volumen como en diversidad, conlleva la necesidad de asegurar la identidad de los usuarios en los accesos locales y remotos a los datos e información contenida en sistemas informáticos o en recintos físicos. La importancia y valor de estos datos motiva a los intrusos a burlar los sistemas de seguridad existentes, lo que obliga a instalar nuevos sistemas cada vez más robustos y confiables. Estas necesidades de autenticación y seguridad, unidas a las que ya existían anteriormente en materia de seguridad de acceso físicos, han determinado un interés creciente por los sistemas electrónicos de identificación y autenticación. Su denominador común es la necesidad de que sean simples, prácticos y confiables.

1.2 Objetivo del estudio

En este estudio se lleva a cabo un análisis de los sistemas biométricos, de las debilidades y fortalezas de cada uno de ellos, haciendo énfasis en el reconocimiento de huellas dactilares, que es una de las técnicas biométricas más populares y económicas.

1.2.1 Objetivo general

El estudio se orienta al análisis de los servicios de acceso e identificación en las diversas plataformas de IT (Information Technology) así como de recintos físicos, todo ello en el marco de ofrecer servicios globales de seguridad en los accesos a través de la biometría. Entre las características principales de esta tecnología se destaca tanto la seguridad como la naturalidad en la interacción hombre-máquina, para así ofrecer un nivel de interacción similar a la que se emplea en la comunicación entre personas. Se comparan las técnicas biométricas como tecnologías para controles de acceso y se ponderan en cada caso las restricciones y beneficios que pueden tener cada una de ellas, frente al grado de seguridad.

1.2.2 Objetivos específicos

- Describir las técnicas biométricas más usadas para el control de acceso e identificación de los individuos.
- Estudiar la aplicabilidad de las técnicas biométricas para verificar la identidad del individuo en los sistemas de control de acceso.
- Analizar la efectividad de las técnicas biométricas basándose en la posibilidad de error de cada una.
- Comparar las características de las técnicas biométricas para así establecer cuál se adecua mejor según las necesidades de los usuarios.

1.3 Justificación

El estudio se centra en la biometría como solución a la problemática de verificar la identidad del individuo en los sistemas de acceso, porque proporciona un alto nivel de seguridad durante el proceso de identificación, debido a que mide de forma unívoca las características humanas.

Casos como la falsificación de documentos de identidad, llevaron a científicos y a la sociedad en general a buscar técnicas biométricas para el reconocimiento y verificación de la identidad.

Muchas de las técnicas iniciales implementadas no eran del todo confiables, o implicaban un gran análisis y estudio, tal es el caso de la huella dactilar, en donde se tenían que comparar las muestras en forma visual. Pero ahora, con el avance de la tecnología, se tiene que estos procesos de identificación y verificación pueden hacerse de manera más eficiente y confiables.

1.4 Limitaciones

Si bien la tecnología biométrica ha ido poco a poco siendo aceptada en Venezuela y en el mundo, su uso se ha limitado hasta ahora solo a servir de control de acceso cuando son requeridos altos niveles de seguridad. Hasta la fecha todavía ningún banco en el país, por ejemplo, emplea sistemas biométricos para identificar sus clientes, aunque en otras partes del mundo este uso ya es ampliamente usado en telecajeros (ATM) por los bancos.

Es difícil hacer una evaluación exacta de todas las tecnologías biométricas mencionadas, ya que la prueba de estos sistemas requiere de laboratorios especiales y un personal entrenado. Este estudio se basa en la literatura disponible, tal como artículos e informes técnicos, estudios evaluativos, folletos de algunos equipos, tesis, notas de prensa y un experimento realizado para engañar un mouse biométrico.

CAPITULO II

REVISIÓN BIBLIOGRÁFICA Y DOCUMENTAL

2.1 Origen y evolución de la biometría

No es verdad que la biometría sea una técnica de identificación futurista, ya que desde hace varios siglos los hombres se han identificado por medio de este sistema. En la época de los faraones, en el valle del Nilo (Egipto) se utilizaban los principios básicos de la biometría para identificar a las personas que realizaban diferentes operaciones comerciales. Muchas son las referencias de personas, que en la antigüedad, han sido identificados por diversas características físicas y morfológicas, como cicatrices, medidas, color de los ojos, tamaño de la dentadura, etc. Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría, al reconocer sus rasgos físicos.

En el siglo XIX comenzaron las investigaciones científicas acerca de la biometría buscando un sistema de identificación de personas con fines judiciales. Con estas investigaciones se produjeron importantes avances y se comenzaron a utilizar los rasgos morfológicos únicos en cada persona para la identificación.

Ya en el siglo XX la mayoría de los países del mundo utilizaba las huellas dactilares como sistema práctico y seguro de identificación. Con el avance tecnológico aparecieron nuevos instrumentos para la obtención y verificación de huellas dactilares. También se comenzaron a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo o la voz.

Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser el mejor método de identificación para seres humanos.

2.2 Concepto y aspectos generales sobre la biometría

La biometría es la ciencia que se dedica al reconocimiento del individuo a partir de sus características anatómicas o rasgos de su comportamiento. Una característica anatómica tiene la cualidad de ser relativamente estable en el tiempo, tal como las huellas dactilares, la silueta de la mano, rasgos faciales, patrones de la retina o el iris. Un rasgo del comportamiento es menos estable, pues depende de la disposición psicológica de la persona, por ejemplo, la firma (Morales, 2000).

Etimológicamente biometría proviene de las palabras *bio* (vida) y *metría* (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona.

La biometría mediante métodos automatizados se encarga de reconocer la identidad de una persona basada en su fisiología (características anatómicas) o en las características de su comportamiento. Se dice que se está reconociendo, cuando las características de un individuo son seleccionadas de un grupo de datos previamente almacenados para identificar un individuo. Así se presume que funciona nuestro cerebro. Aunque este proceso para el cerebro es relativamente rápido y eficiente, se puede convertir en un proceso bastante lento al ser procesado por una computadora. Muchos son los parámetros que hay que identificar y a medida que crecen los datos previamente almacenadas y el nivel de confidencialidad exigido, más será el tiempo que tomará para reconocer a una persona.

También es importante afinar el significado de las palabras "fisiología de una persona" y "características de su comportamiento". La fisiología de una persona, es decir sus características anatómicas, son aquellos aspectos relativamente estables durante el transcurso de la vida de un individuo, tales como huellas dactilares, patrón

de iris, patrón de los capilares ubicados en la parte posterior del ojo, entre otros. En cambio la característica del comportamiento es más bien el reflejo de la psicología de una persona. La firma, la manera de utilizar un dispositivo y la voz, son ejemplos de las características de comportamiento más comunes. Debido a la ausencia de estabilidad de estas características, los dispositivos deben ser automáticamente ajustados con los nuevos patrones de referencia pero con el tiempo, es decir que el dispositivo será capaz de amoldarse a la persona.

Debido a que la biometría tiene una gran variedad de aplicaciones, es muy difícil establecer una definición completa que abarque a todas. La biometría física se basa en medidas y datos derivados de una parte del ser humano. La huella dactilar, el iris, la retina y la cara son las características físicas más utilizadas en biometría.

Las características del comportamiento se basan en acciones realizadas por una persona. En este sentido, la biometría del comportamiento se basa en medidas y datos derivados de una acción, e indirectamente de las características físicas que lo han generado. El reconocimiento de la voz, del tono de voz y de la firma son las medidas biométricas de comportamiento más utilizadas.

Es importante remarcar que la distinción entre físico/comportamental es algo difusa. La biometría del comportamiento se basa en parte en características físicas, como por ejemplo la forma de pronunciar las vocales. La biometría basada en características físicas también depende del comportamiento, tal como la manera en que la persona coloca su dedo o mira a la cámara. Sin embargo, la distinción entre biometría física y comportamental es útil para entender cómo funciona la biometría y cómo puede aplicarse al mundo real.

La medición biométrica se ha venido estudiando desde hace algún tiempo y es considerada en la actualidad como el método ideal de identificación humana. La identificación por medio de las huellas dactilares constituye una de las formas más

comunes de la utilización de la biometría. Una huella dactilar está formada por una serie de surcos. Las terminaciones o bifurcaciones de los mismos son llamados “puntos de minucia” y cada uno de estos puntos tiene una característica y una posición única, que puede ser medida. Comparando esta distribución es posible reconocer la identidad de una persona que intenta el acceso a un sistema.

2.3 Indicadores biométricos

Un indicador biométrico es alguna característica con la cual se puede aplicar la biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos:

- Universalidad: toda persona posee esa característica.
- Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy baja (casi nula).
- Permanencia: la característica no cambia significativamente en el tiempo.
- Cuantificación: la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a una característica como indicador biométrico. Luego de seleccionar algún indicador biométrico que satisfaga los requerimientos antes señalados, es necesario conocer las restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores.

2.4 Proceso de identificación personal

Cualquier proceso de identificación personal puede ser analizado mediante un modelo simplificado. Este postula la existencia de tres indicadores de identidad que definen el proceso de identificación (Morales, 2000):

- Conocimiento: la persona conoce algo (por ejemplo: un código)
- Posesión: la persona posee un objeto (por ejemplo: una tarjeta).
- Característica: la persona tiene una característica que puede ser verificada (por ejemplo: color de ojos).

En la figura 1 se pueden observar los tres indicadores del modelo de identificación personal y se detalla la identificación de características, con algunos ejemplos.

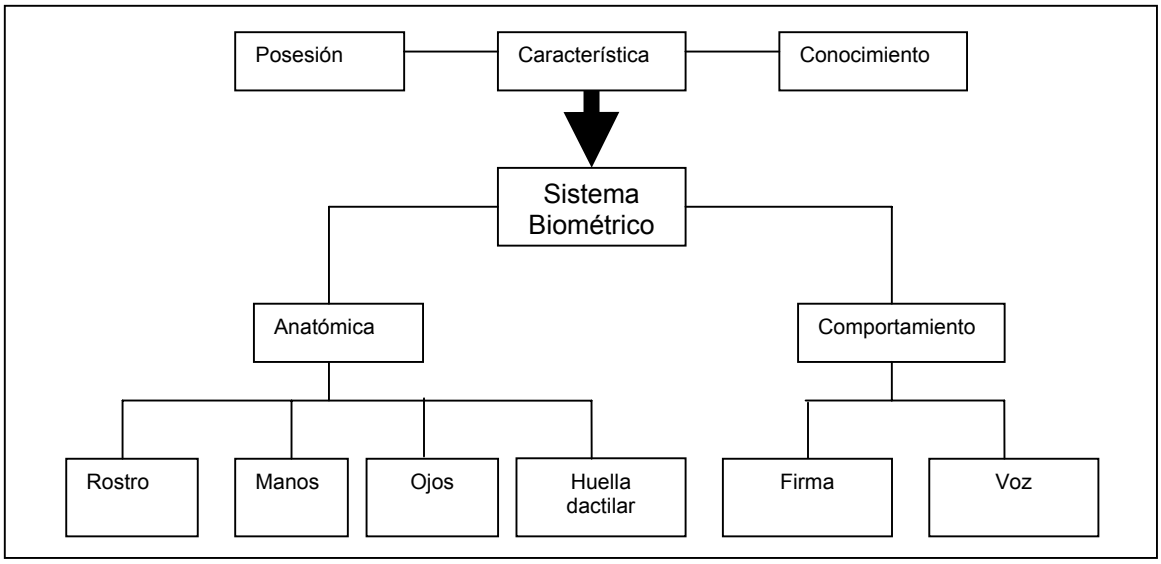


Figura 1. División de las características biométricas dentro del modelo de identificación personal (Morales, 2000)

Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal. Además, pueden ser combinados con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección.

Distintas situaciones requerirán diferentes soluciones para la labor de identificación personal. Por ejemplo, con relación al grado de seguridad, se debe considerar el valor de lo que está siendo protegido así como los diversos tipos de amenazas que pudieran surgir. También es importante considerar la reacción de los usuarios y el costo del sistema.

Existen distintos métodos y técnicas de identificación entre los cuales se encuentra la biometría, que se basa en el tercer indicador, y se ha transformado en un área importante en lo referente a identificación (Miller, 1994).

2.5 Técnicas biométricas utilizadas en la identificación del individuo

El reconocimiento biométrico responde a un sistema automático basado en el reconocimiento de patrones, que permite la identificación y/o verificación de la identidad de personas a partir de características morfológicas o de comportamiento, propias y únicas del individuo. Asimismo, la naturaleza del tipo de característica, (morfológica o de comportamiento), se encuentra directamente relacionada con el grado de variación de las mismas con el paso del tiempo, siendo muy inferior en el primer caso que en segundo, ya que como sabemos, el comportamiento está íntimamente relacionado con factores psicológicos y éstos sí son función directa del tiempo.

En la actualidad existen diversas tecnologías para la identificación o reconocimiento biométrico. A continuación se listan la más conocidas:

- Reconocimiento por medio de la huella dactilar.
- Reconocimiento por medio de la mano.
- Reconocimiento facial.
- Reconocimiento por medio de la retina.
- Reconocimiento por medio del iris.
- Reconocimiento de la voz (que no se debe confundir con el reconocimiento de la pronunciación).
- Reconocimiento de la firma.
- Reconocimiento del modo de escribir en un teclado.

Existen otras tecnologías menos difundidas, como son:

- Reconocimiento del ADN.
- Reconocimiento de la forma de la oreja.
- Reconocimiento del olor humano.
- Reconocimiento de la forma de las venas (de la parte superior o inferior de la mano)

Cada una de las técnicas anteriores posee ventajas y desventajas, las cuales deben tomarse en consideración al momento de decidir qué técnica utilizar para una aplicación específica.

Todas las soluciones biométricas mencionadas anteriormente garantizan la privacidad de los usuarios, puesto que no almacenan los elementos mismos de caracterización de una persona (por ejemplo: la huella dactilar o la imagen de la cara), sino una representación digital de los atributos correspondientes.

2.5.1 Proceso de reconocimiento por medio de huellas dactilares

El proceso de reconocimiento por medio de huellas dactilares consiste en tomar ciertas características de las huellas dactilares del individuo (ver anexo 1), convertir la lectura electrónica a un código digital y compararlo con los existentes en la base de datos (ver figura2). Este método tiene sus limitaciones, ya que las lecturas pueden complicarse (por suciedad, grasa, quemaduras, cicatrices, etc. que presente el individuo en su dedo) de tal manera que pueden alterar la imagen captada y provocar un falso negativo cuando el sistema la compara con la imagen almacenada en la base de datos (ver Figura 3). Sin embargo existen sistemas más modernos que capturan otros detalles, aunque a costa de ocupar mayor espacio de almacenamiento (Gómez y Ormella, 1999).

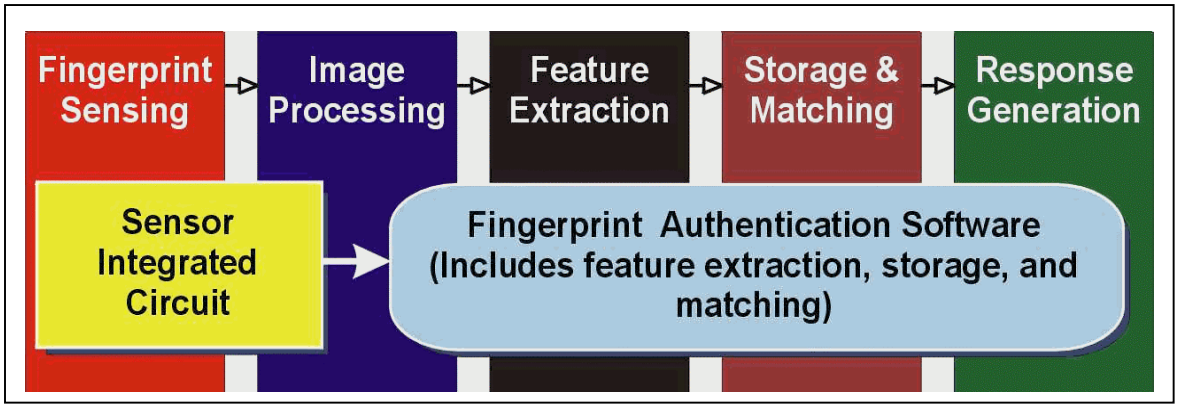


Figura 2. Diagrama de bloque de un sistema de reconocimiento de huella dactilar (Olguín, 1999)

Entre los usos de este sistema se pueden mencionar el acceso a instalaciones físicas, acceso a redes, estaciones de trabajo y recursos de red, entre otros. La operación de un sistema de este tipo puede incluir el escaneado de los dedos desde diferentes ángulos para así tener una información más completa.

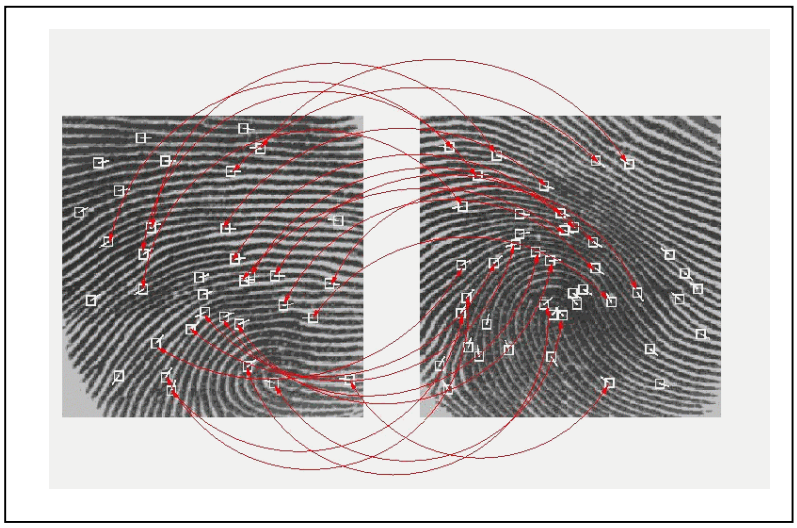


Figura 3. Proceso de comparación. (Olguín, 1999)

La información en sí misma consiste en establecer dos componentes: patrón y detalles. El patrón se refiere a las crestas y valles que conforman la huella dactilar, así como un conjunto de detalles, tales como los lugares en que las líneas se cortan o bifurcan, etc. Los patrones básicos son tres: lazo, arco y espiral. En un patrón tipo lazo, las líneas comienzan de un lado del dedo, llegan hasta un tope aproximadamente en el centro y regresan hacia el mismo lado. En un patrón en forma de arco, las líneas también comienzan al costado del dedo y llegan al centro pero ahora siguen hacia el otro lado del dedo, formando precisamente un arco que pasa por la zona central. Finalmente, en un patrón en forma de espiral las líneas forman círculos aproximadamente concéntricos en el centro del dedo (ver figura 4). En muchos casos, las huellas dactilares muestran una combinación de estos patrones (Gómez y Ormella,1999).

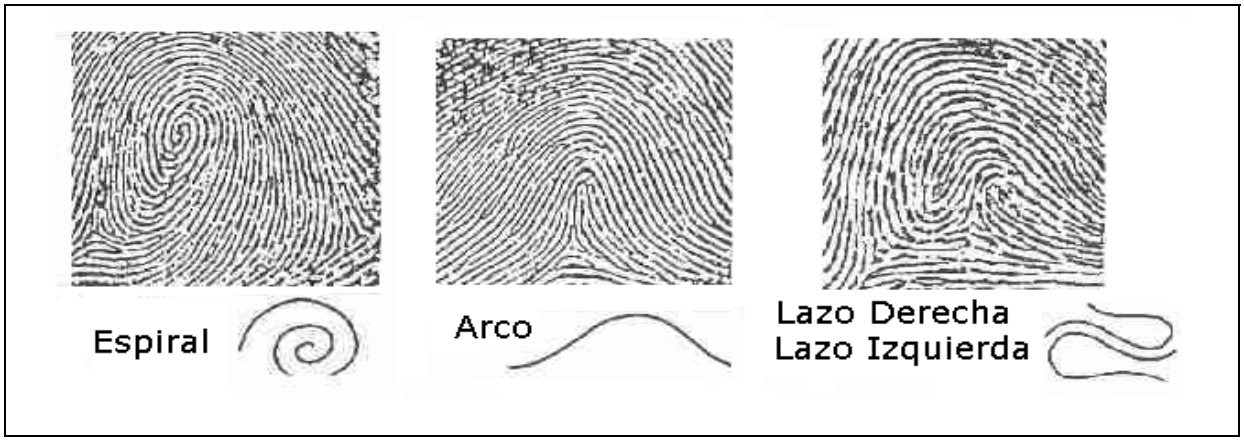


Figura 4. Patrones básicos que conforman la huella dactilar.

El otro componente mencionado se refiere a los detalles, en la práctica tan importantes como los patrones. Aquí se trata de determinar dónde aparecen puntos singulares en las líneas, es decir, detalles como la terminación, ruptura, formación de un punto y cambios en general de las líneas (ver figura5). En este aspecto podemos distinguir:

- **Bifurcación**: El punto donde una línea se divide en varias líneas llamadas ramas.
- **Divergencia**: El punto donde se separan varias líneas prácticamente paralelas.
- **Cercado**: Punto en que una línea que se divide en dos ramas que más adelante se vuelven a juntar.
- **Terminación**: Donde termina una línea.

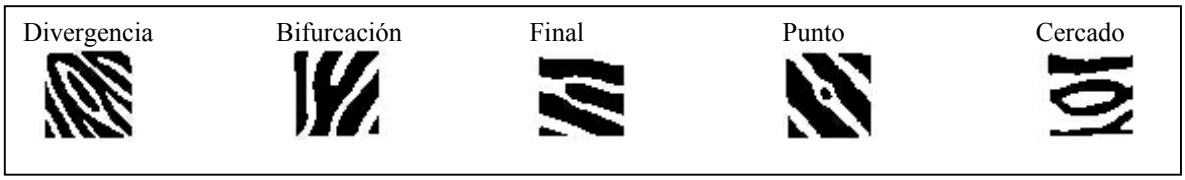


Figura 5. Ejemplo de algunos detalles que se encuentran en la huella dactilar. (Olguín, 1999)

Cada uno de los detalles mencionados se posiciona en un sistema de ejes coordenados x,y registrándose, entre otras características, la curvatura de las líneas y el espacio entre las mismas en el punto singular como se muestra en la figura 6.

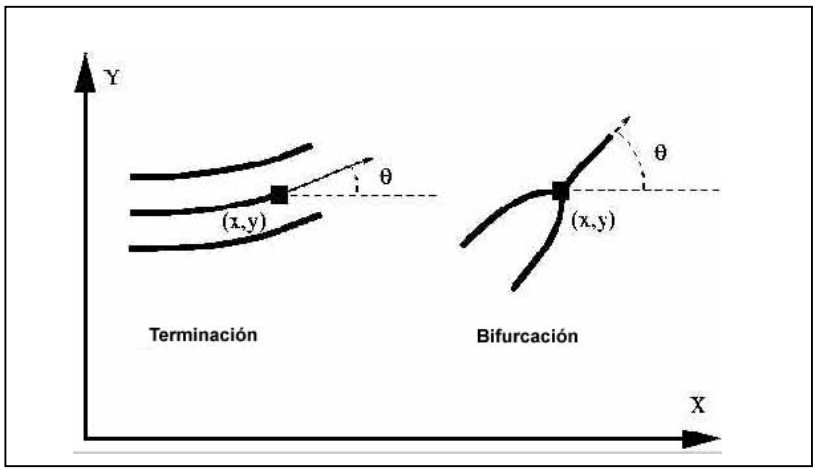


Figura 6. Ejemplo de un sistema de ejes coordenados x,y de los detalles: terminación y bifurcación.

Una vez obtenida la huella digital, los algoritmos de los sistemas automáticos de reconocimiento de huellas dactilares siguen tres pasos (Lozano, 2002):

- Filtrado de huellas dactilares.
- Extracción de las características fundamentales.
- Reconocimiento de la huella dactilar.

El objetivo del filtrado es poder obtener una imagen digital (de ceros y unos) que luego pueda ser tratada con facilidad por el resto de los módulos. Por otra parte utilizar un determinado nivel de luminosidad para definir cada punto de la imagen como blanco o negro, no da buenos resultados ni siendo dicho nivel de luminosidad calculado previamente (umbral dinámico).

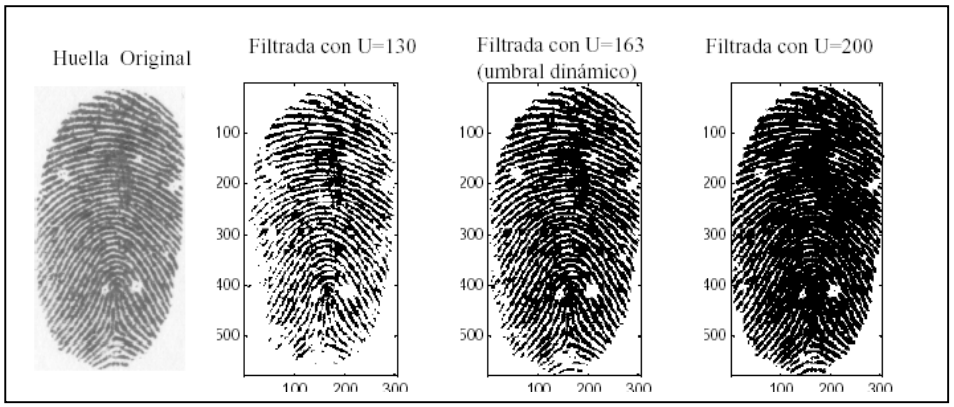


Figura 7. Filtrado de la huella dactilar. (Lozano, 2002)

Por todo ello, ha sido necesario desarrollar algoritmos de filtrado especializado en las huellas dactilares. Fundamentalmente se basan en la determinación de direcciones de cada punto de la huella digitalizada sin binarizar (ver figura 7). Para ello se utiliza el proceso de convolución y para cada zona de la imagen una mascara de filtrado con la orientación que siga las crestas y valles de la zona (ver figura 8).

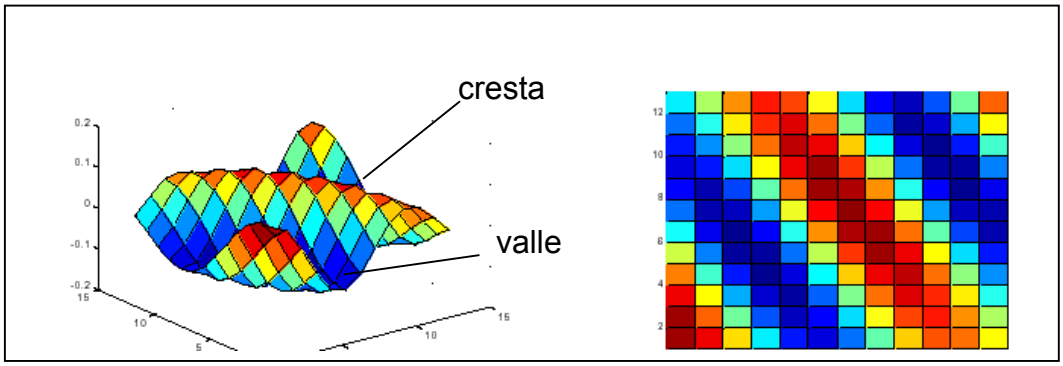
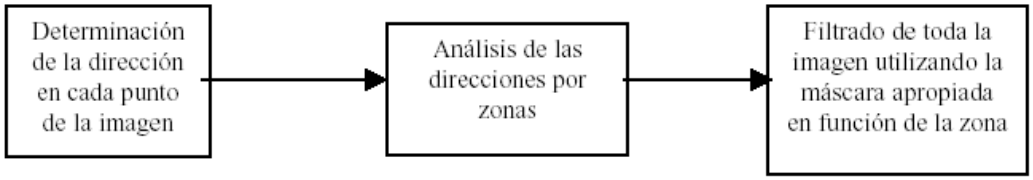


Figura 8. Ejemplo del proceso de filtrado para 135º (Lozano, 2002)

El proceso general de filtrado se realiza en tres etapas:



Para la extracción de las características, los algoritmos existentes permiten clasificar la huella en cinco clases:

- Espiral.
- Lazo Derecho.
- Lazo Izquierdo.
- Arco.

Estos algoritmos separan el número de crestas presentes en cuatro direcciones (0°, 45°, 90° y 135°) mediante un proceso de filtrado de la parte central de la huella (ver figura 7).

Los sistemas de identificación, es decir, de reconocimiento de un individuo entre muchos, son conocidos como AFIS (por las siglas en ingles de Sistemas de Identificación Automática de Huellas Dactilares). A su vez hay dos tipos de aplicaciones AFIS: forense y civil. En el primer caso se capturan múltiples imágenes de cada dedo desde diferentes ángulos. Las aplicaciones civiles, en cambio, trabajan generalmente con una única imagen plana de algún dedo.

Actualmente tres son las tecnologías usadas para el reconocimiento de huellas dactilares: óptica, capacitiva o basada en chips y ultrasonido.

El reconocimiento por medios ópticos es el más viejo y depurado. La tecnología por dispositivos ópticos consiste en capturar la imagen refractada de una fuente de luz. El usuario toca una placa de vidrio que trae el dispositivo con el dedo (usualmente el pulgar) donde se proyecta la luz que se genera desde adentro del dispositivo. Luego esta luz brilla sobre las partes del dedo que interesan y se captura esta luz que es convertida en imagen a procesar. La captura de la imagen se hace por medio de un sensor basado en un CCD (Dispositivo Acoplado por Carga) similar a los que se usan en escáneres y cámaras digitales (ver figura 9).

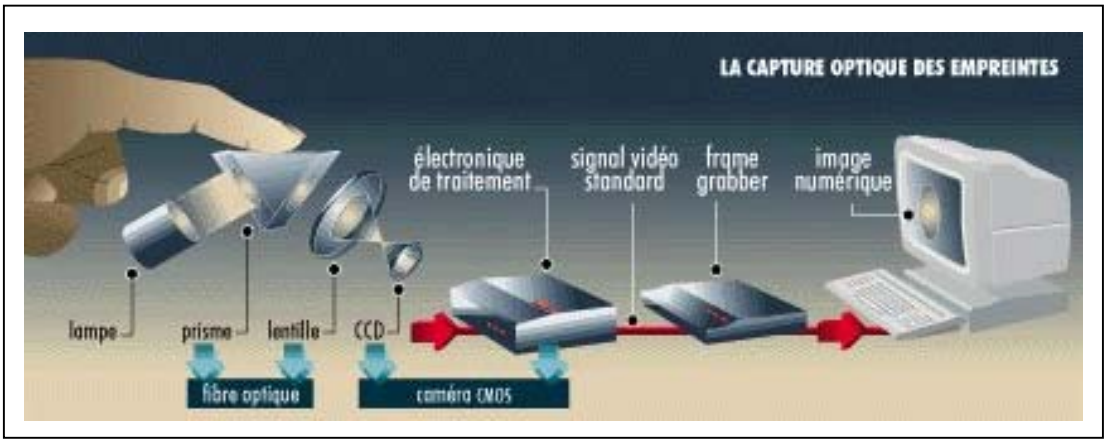


Figura 9. Captura de la huella digital mediante un dispositivo óptico. (Toptrend Technologies Corp., 2001)

Además de la sensibilidad del dispositivo e irregularidades posteriores al registro inicial, el método óptico puede resultar particularmente sensible a la presencia de grasa y suciedad en general. El hecho es que estos cuerpos extraños van dejando en la placa una huella fantasma (llamada imagen latente u oculta) que, con el tiempo, pueden afectar la exactitud del dispositivo. Para compensar este efecto, algunos fabricantes guardan en memoria la imagen latente de la última huella de modo que al tomar la siguiente la "restan" de la nueva imagen obtenida.

Por su parte, el sistema capacitivo consiste en establecer un campo eléctrico entre dos componentes aislados eléctricamente, en este caso el dedo y un chip (ver figura 10). La información resulta de las variaciones del campo eléctrico en los diferentes puntos enfrentados. Este sistema es más preciso que el anterior porque las mediciones del campo eléctrico pueden diferenciar crestas de valles (como si fuera una imagen tridimensional), pero el contacto con el chip puede desgastarlo con el tiempo.

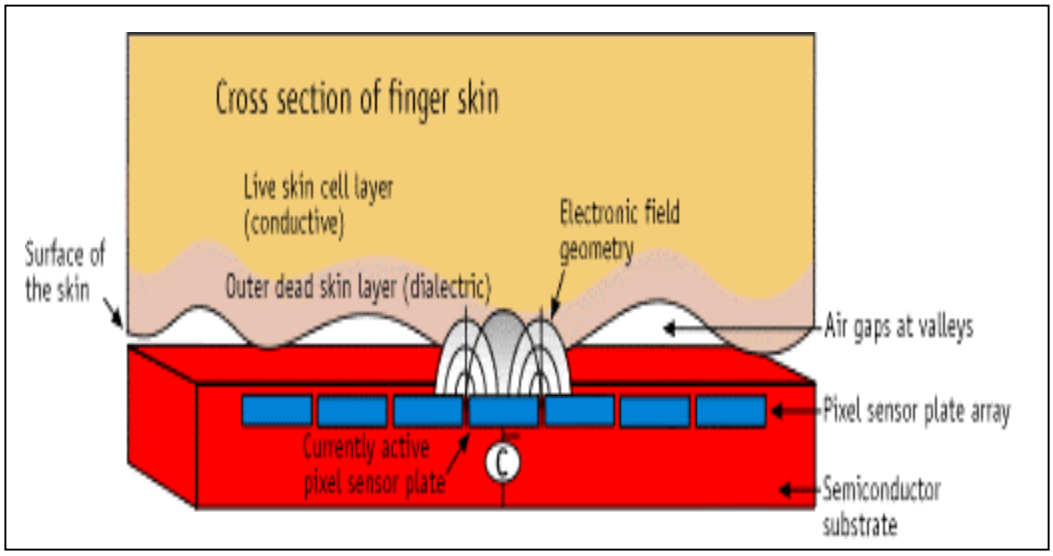


Figura 10. Sensor capacitivo clásico. (Olguín, 1999)

Existen otros sistemas capacitivos que utilizan las técnicas táctiles o termales las cuales usan un sofisticado chip de silicon sensible a la presión o al calor que

capturan la imagen. Las imágenes termales también pueden descartar si lo que se lee es una huella artificial, ya que se identifica el calor capturado con el corporal.

Buscando lo mejor de cada sistema, se han desarrollado combinaciones de ambos. Pero lo más novedoso es el reconocimiento de huellas dactilares por medio del ultrasonido (ver figura 11). En este caso se coloca el dedo sobre una placa pero sin necesidad de tocarla. Se transmiten ondas acústicas y se calcula la distancia basada en la impedancia del dedo, la placa lectora y el aire. Tampoco hace falta iluminarla, porque simplemente se miden los ecos de una emisión de ultrasonido que proviene desde abajo de la placa. El ultrasonido es capaz de penetrar la suciedad y los residuos sobre la placa y el dedo, mejorando así los problemas de la tecnología óptica. La tecnología por ultrasonido, a pesar de ser considerada como la más confiable en cuanto a reconocimiento dactilar, no es muy utilizada actualmente debido a sus altos costos.

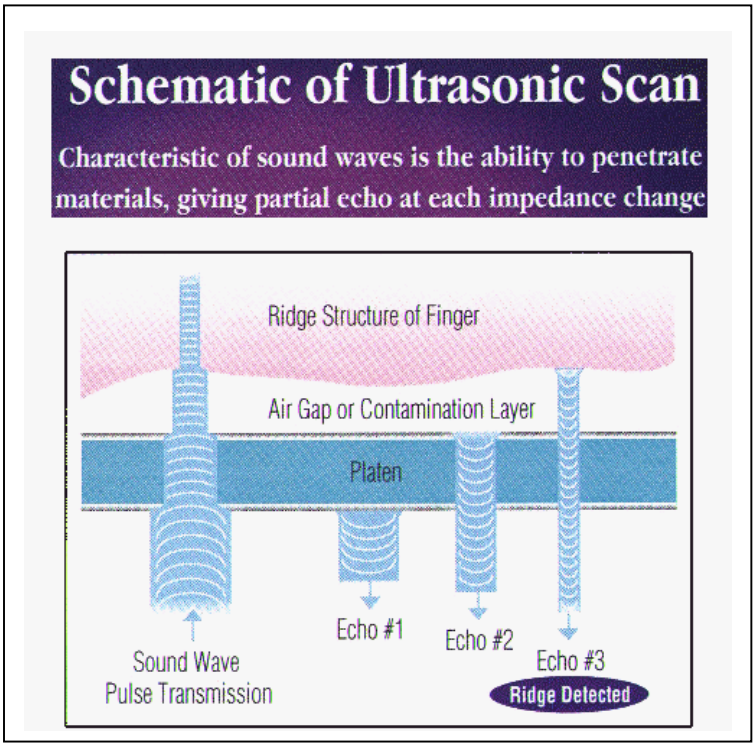


Figura 11. Transmisión y reflexión de ondas de sonido. (Jaypeetex Engineering, 2001)

2.5.2 Proceso de reconocimiento por medio de la geometría de la mano

En una operación de poco más de un segundo, un sistema de este tipo permite obtener un registro tridimensional de las principales características de la mano y/o los dedos tales como longitud, ancho y altura, algunas áreas particulares, etc. así como posiciones relativas de dedos, nudillos, etc. Con esa información, el sistema crea un mapa tridimensional del contorno de la mano que luego transforma a un código de unos cuantos bytes. En la práctica, sin embargo y con los productos actuales, no se alcanza el nivel de eficiencia logrado con otros sistemas biométricos. Además, el análisis puede verse afectado por heridas, desgarros e hinchazones. (Gómez y Ormella, 1999).

Los sistemas de geometría de extremidades responden a tres variantes diferentes con su propia tecnología especialmente de hardware: geometría de las manos, de un dedo y de dos dedos.

El primer sistema trabaja colocando la mano sobre una placa que tiene guías para ubicar cada uno de los dedos. La cámara toma una fotografía estableciendo hasta casi un centenar de características diferentes.

Para los sistemas de geometría de dedos, el dispositivo de captura tiene un pequeño pistón donde se ubica el dedo. El sistema tiene en su parte interna un conjunto de pequeñas ruedas que se mueven alrededor del dedo cuando éste empuja el pistón. De esta manera se levantan mediciones de secciones diferentes a lo largo de unos cuatro centímetros del dedo.

Usualmente, el sistema de dos dedos trabaja con el dedo índice y el del medio o corazón.

En esta categoría también es usual incluir el reconocimiento de la palma de la mano por medio del escaneado correspondiente, que se analiza luego de manera similar al reconocimiento de huellas dactilares ya comentado.

2.5.3 Proceso de reconocimiento por medio de la cara

Este método tiene la ventaja que no es intrusivo para el usuario y puede almacenar directamente fotos digitales, sin embargo, a veces se requieren cámaras muy complejas y aún así el sistema no es totalmente seguro con respecto a falsos positivos (falsas aceptaciones). Por otra parte las caras cambian con el tiempo, limitación que al menos puede requerir actualizaciones periódicas.

Los productos de este tipo trabajan con varias imágenes de cada usuario y el proceso de reconocimiento está regido por una serie de reglas que conducen a una identificación efectiva. Tanto es así que algunos usan tecnología de redes neuronales propias de un esquema de inteligencia artificial que básicamente adquieren conocimiento de la experiencia. De esta manera, siguiendo un proceso de aprendizaje, un sistema biométrico de estas características puede ir reduciendo sistemáticamente la cantidad de variables de análisis faciales que se encuentran almacenadas en la base de datos para encontrar similitudes con la cara escaneada.

La cámara puede estar en algunos casos a un metro o poco más de distancia. En general la captación es en movimiento para que no se pueda usar una foto tratando de engañar al sistema. En otros casos se trabaja con vistas de frente y de perfil.

En la imagen capturada se analiza la geometría de la cara con parámetros tales como la distancia entre los ojos y la nariz, curvatura de los huesos, asimetrías de puntos notables, etc. Estos sistemas están diseñados para compensar el efecto de barbas, lentes o anteojos y sombreros. Sus principales usos se orientan a la verificación de una persona determinada (identificación del usuario de una

computadora personal) y al reconocimiento de un individuo entre muchos (identificación de terroristas en aeropuertos).

La primera etapa consiste en la detección de la imagen capturada de la cual se separan los elementos faciales eliminando información extraña (como la barba y anteojos).

El software luego analiza la imagen buscando determinar las estructuras típicas de los elementos más importantes (como ojos y nariz) con las que construye la cara completa recortando el fondo original y ubicándola dentro de un recuadro rectangular llamado máscara binaria.

La segunda etapa es la del reconocimiento o comparación de la imagen resultante con las de la base de datos.

El análisis de las características faciales se realiza por medio de operaciones matemáticas recursivas para encontrar los componentes únicos o propios de la muestra. De esta manera la imagen se descompone en un conjunto de áreas de luz y sombras dentro de un determinado patrón. El resultado es una cara que resulta ser la combinación de las áreas únicas de esa imagen.

También se puede trabajar con imágenes térmicas logradas con cámaras infrarrojas que permiten crear mapas de venas subcutáneas. Estos sistemas resultan más precisos especialmente por no depender de cambios en la superficie de la piel y por supuesto, pueden llegar a operar en la oscuridad.

La fase final del reconocimiento comparará las características únicas encontradas con las características correspondientes de la base de datos. (Gómez y Ormella, 1999)

2.5.4 Proceso de reconocimiento por medio del iris y la retina

La investigación en la tecnología de la identificación ocular comenzó en el año 1935. Durante ese año apareció un artículo del 'New York State Journal of Medicine' que sugirió que el patrón de las arterias y venas de la retina podría ser usado para la identificación univoca de un individuo.

En 1993 el Dr. J. G. Daugman de la Universidad de Cambridge en Inglaterra, desarrolló las fórmulas matemáticas usadas para medir las características que varían en el iris. Solamente en el iris hay más de 400 características distintivas, que pueden ser cuantificadas y usadas para identificar a un individuo. En la práctica se usan aproximadamente 260 de estas características, algunas de las cuales son: surcos de contracción, estrías, huecos, fibras de colágeno, filamentos, anillos y manchas negras. El iris provee un robusto método de identificación debido a que se mantiene inalterable con el pasar del tiempo.

Por otro lado la identificación por medio de la retina está basada en los patrones que contienen las arterias y venas que están en la parte de atrás del ojo.

Los sistemas basados en la identificación a través del iris o la retina de las personas generalmente son los que ofrecen mayor seguridad entre los métodos biométricos (ver figura 12), gracias a la característica de singularidad de los patrones y a la calidad de los dispositivos de captura, (se utiliza una cámara de video para capturar los patrones de los tejidos del iris o las venas de la retina). Estos sistemas son iguales en muchos aspectos porque ambos exploran el ojo, pero diferentes porque cada uno se centra en una parte única del ojo. A continuación se explica cada uno:

Reconocimiento por medio del iris:

El iris es la franja de tejido que rodea la pupila del ojo. Tiene una estructura compleja de estrías, anillos, surcos, coronas y flecos que ofrece prácticamente

infinitas variaciones incluso entre ambos ojos de la misma persona y que además permanece constante con el tiempo.

El reconocimiento del iris es una de las tecnologías de identificación más precisa. Es altamente escalable y extremadamente estable. El reconocimiento del iris ofrece una identificación de la más alta tecnología, capaz de reemplazar códigos secretos, contraseñas y signos. El pionero de este proceso científicamente probado y operacionalmente confiable es John Daugman, Ph,D. Universidad de Cambridge, Inglaterra.

Los irises no son idénticos, ni entre derecho e izquierdo en la misma persona y ni siquiera entre mellizos idénticos. La abundancia en detalles del iris y la accesibilidad de la imagen convierten al iris en el mejor método de identificación personal. El reconocimiento del iris está compuesto de cuatro elementos:

1. Adquisición de la imagen del iris
2. La implementación de software que desarrolla el código para cada iris
3. Una plataforma computacional que ejecuta el software
4. Una manera de mostrar la información referente al registro y el reconocimiento

La médula de la tecnología del reconocimiento del iris es el software que ejecuta las siguientes funciones:

1. Adquiere una imagen del iris
2. Define los limites del iris
3. Establece un sistema de coordenadas del iris
4. Define unas zonas de análisis dentro del sistema de coordenadas
5. Analiza los datos de la imagen
6. Genera un código de 256 a 512 bytes (típicamente)
7. Cifra y guarda el código.

La identificación basada en el reconocimiento de iris consiste en capturar una imagen del iris en blanco y negro, en un entorno correctamente iluminado y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas (McMordie, 1997), hasta obtener una cantidad de datos suficiente para los propósitos de autenticación. Esa muestra, es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todas las técnicas biométricas.

El iris se ve afectado por la pupila cuando ésta reacciona a la luz. Las deformaciones elásticas que ocurren con la dilatación y contracción son rápidamente corregidas empleando algoritmos matemáticos que se encargan de localizar los bordes interno y externo del iris (Olguín, 1999).

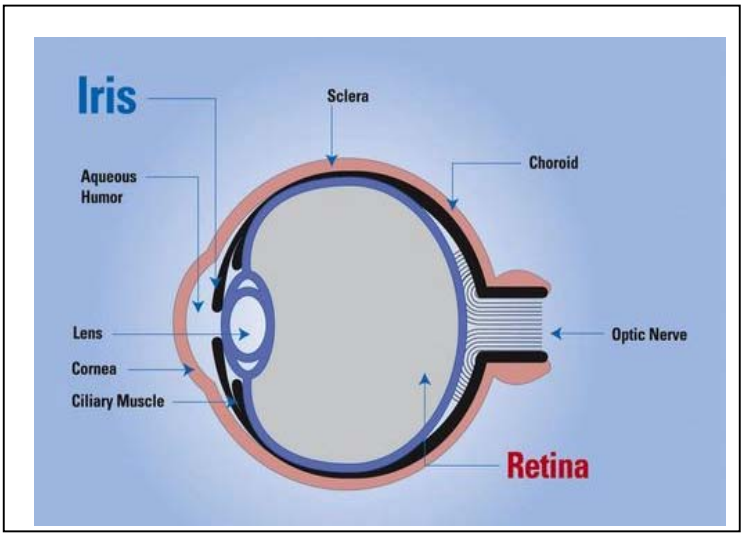


Figura 12. Iris y retina del ojo

Los datos capturados se procesan por medio de complejos algoritmos matemáticos (ver figura 13). Esto implica que para una gran cantidad de muestras se necesita gran capacidad de almacenamiento.

Las implementaciones de sistema de identificación por medio del iris responden a dos tipos: activo y pasivo. La forma activa requiere que el usuario se mueva hacia atrás y adelante de manera tal que la cámara pueda ajustar el foco en el iris del usuario. El sistema activo requiere que el usuario se localice entre 15 y 35 centímetros de la cámara. El sistema pasivo es diferente debido a que incorpora una serie de cámaras que localizan y enfocan el iris. El sistema pasivo permite al usuario a estar hasta un metro y medio de la cámara.

La identificación del iris puede ser dividida en cuatro pasos. Primero, el usuario se sitúa en frente del sistema de identificación, mientras una cámara gran angular calcula la posición del ojo. Una segunda cámara hace zoom al ojo y toma una fotografía en blanco y negro. Después el sistema aplica a la imagen una grilla de factores de corrección o factores de filtrado e identifica los sectores brillantes y oscuros. El propósito de esta grilla es para que el sistema reconozca patrones en el iris y pueda generar 'puntos' a través de estos patrones, para convertirlos en una huella ocular. Finalmente, esta huella es comparada contra referencias guardadas en una base de datos.

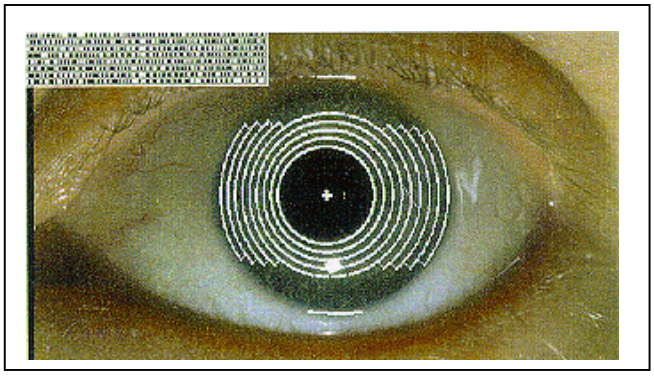


Figura 13. Mapa del Iris. En la parte superior se aprecia el código generado.

El tiempo que el sistema necesita para reconocer el iris de un individuo es de aproximadamente 2 segundos. Un código de una plantilla de referencia puede ocupar alrededor de 256 a 512 bytes. Esta pequeña plantilla proporciona una ventaja cuando de búsquedas en base de datos se trata. Como resultado hasta 100.000 registros pueden ser comparados por segundo en una PC estándar.

Reconocimientos por medio de la retina:

La retina es la capa más interna llena de vénulas o venillas de la pared posterior del globo ocular. La retina también permanece bastante estable con el tiempo salvo cuando resulta afectada por algunas enfermedades.

Con una imagen adecuada se puede establecer un mapa muy preciso y único del patrón de conductos venosos.

El barrido de la retina involucra a un haz de rayos infrarrojos de baja intensidad que se proyecta a través de la parte de atrás del ojo en la retina. Se usa luz infrarroja debido a que las arterias y venas de la retina absorben la luz infrarroja más fácilmente que el tejido que las rodea. Esta luz es reflejada por la retina de vuelta en la cámara. Se captura este patrón retinal y se convierte en un código de bytes para compararlo con los almacenados en la base de datos, si coincide con uno de los códigos almacenados, se permite el acceso. (Gómez y Ormella, 1999)

2.5.5 Reconocimiento por medio de la autenticación de la voz

La voz es una forma natural de comunicación que es persuasiva, eficiente y puede ser usada a distancia. El primer sistema de reconocimiento de voz fue desarrollado en 1952 sobre una computadora analógica usando voz discretizada para reconocer los dígitos del 0 al 9 con un algoritmo de plantilla de concordancia dependiente de la persona que habla, reportando en el reconocimiento una exactitud de 98% (Davis y Col., 1952). Más tarde en esa misma década, un sistema con atributos similares fue desarrollado, el cual reconocía consonantes y vocales (Dudley, 1958). En los años sesenta la investigación en reconocimiento de voz se centró en las computadoras digitales. Esta plataforma proporcionó las bases para la tecnología de reconocimiento de voz como se conoce hoy en día (Lea, 1980). A pesar del rápido progreso inicial, las limitaciones en arquitecturas de computadoras previnieron cualquier desarrollo comercial de sistemas de reconocimiento de voz. No obstante que la tasa de transferencia de datos de voz es solamente alrededor de 50

bits por segundo, los requerimientos computacionales asociados en la extracción de esta información son enormes. En la última década, sin embargo, un número de sistemas comerciales ha sido exitosamente desarrollado (Buyer, 1993). Por lo tanto, un sistema exitoso de voz debe permitir tener en cuenta las limitaciones de la tecnología actual. Estas limitaciones incluyen la dependencia de la persona que habla, la continuidad de voz y el tamaño del vocabulario.

Los sistemas independientes de la persona que habla, pueden reconocer voz de cualquier persona. Los sistemas dependientes de la persona que habla, deben ser entrenados para cada usuario individual. También existen los sistemas adaptables a la persona que habla, el cual registra plantillas independientes de la persona que habla y las adapta a usuarios específicos. Los sistemas de voz continuos pueden reconocer palabras habladas en un ritmo natural mientras que los sistemas de palabras aisladas requieren de una pausa deliberada entre cada palabra. No obstante, los sistemas de voz continúan siendo más difíciles de procesar por la dificultad en detectar los límites de cada palabra. El tamaño del vocabulario puede variar de 20 palabras a más de 40,000 palabras. Los grandes vocabularios causan dificultades en mantener exactitud, pero los pequeños pueden imponer restricciones no deseadas sobre la naturalidad de la comunicación. A menudo el vocabulario debe ser restringido por reglas gramaticales las cuales identifican como las palabras pueden ser habladas en el contexto (Peacocke, 1990).

En la voz que se registra se analizan principalmente el tono, la intensidad y la frecuencia de los sonidos, así como las inflexiones o cadencia en el hablar y el propio comportamiento lingüístico.

Para el registro inicial generalmente se repite varias veces una misma frase o una serie de frases. De esta manera se establece una plantilla individual contra el cual se compara cada vez que se recurra al sistema para verificación del usuario.

La exactitud del sistema puede verse afectada principalmente por el ruido de fondo y las características del elemento que capta el sonido (teléfono mismo o un micrófono), así como por variaciones naturales como cambios de humor, fatiga, transcurso del tiempo, etc. Además, ocupa bastante espacio de almacenamiento.

2.5.6 Reconocimiento por medio de la firma

Un sistema VDF (Verificación Dinámica de Firmas) pondera y mide características de la firma, especialmente las relacionadas con el modo cómo se firma. Algunas de las características analizadas son la presión que se ejerce sobre la lapicera en las diferentes partes, puntos en que la lapicera se separa del papel, orden, velocidad y aceleración de los trazos y agudeza de los lazos (Villalón, 2002).

Para medir características (tal como la aceleración) se necesita identificar los trazos en planos de ejes coordenados con una resolución de fracción de milímetro que se muestrean periódica y sincrónicamente (ver figura 14).

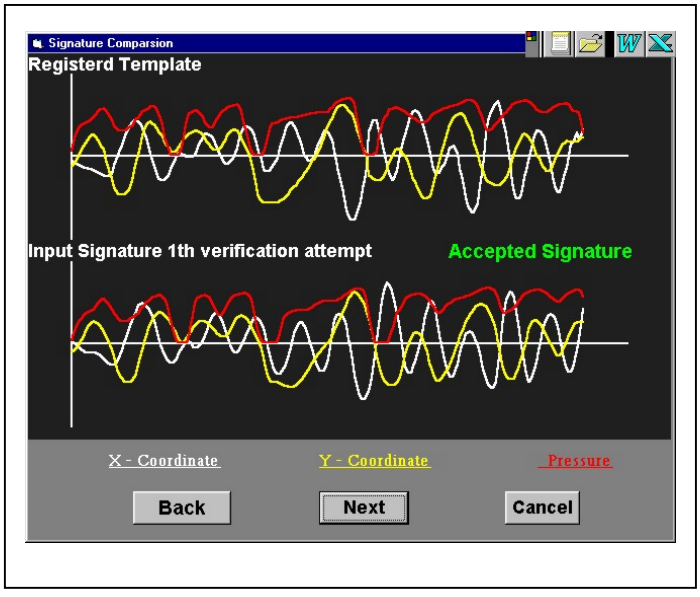


Figura 14. Verificación de la firma por un eje de coordenadas.

La representación matemática de todas las características se guarda adecuadamente codificada para ser tomada como base cada vez que se recurra al sistema.

Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el sistema es capaz de distinguir como auténtica.

Algunas limitaciones de este sistema se refieren a que los cambios naturales que se producen en las firmas con el tiempo, pueden aumentar el nivel de rechazos equivocados.

2.5.7 Otros sistemas

El sistema de dinámica del tecleado sobre un teclado de computadora también permite reconocer a un individuo por medio de características del comportamiento, esta solución trabaja con dos métricas: por un lado se captura el tiempo de residencia, es decir el tiempo que permanece apretada cada tecla, y por el otro el tiempo de vuelo, es decir el tiempo invertido en pasar de una tecla a otra. De esta manera puede obtenerse una medida del ritmo de cada usuario. Generalmente se trabaja con una palabra o frase corta que el usuario repite varias veces al momento del registro inicial, muestras contra las que se harán las comparaciones posteriores. (Ruggles, 1998).

Otras investigaciones no han salido del laboratorio o están en las primeras etapas de desarrollo como son: la medición de venas del cuerpo por medio de luz

infrarroja, el mapeo de los poros de la piel y el análisis de la composición del olor corporal (Davis, 1997).

2.6 Procedimiento de uso de las tecnologías biométricas

A continuación se describen sucintamente algunos procedimientos de uso:

- **Reconocimiento por medio de la huella dactilar**: el usuario ha de colocar el dedo encima de la superficie del escáner óptico, del chip o de la placa. El escáner, el chip o la placa forman parte de un dispositivo periférico (en un ratón, teclado etc.). El usuario debe mantener su dedo sobre la superficie del escáner, chip o placa durante 1-2 segundos, mientras el sistema realiza una comparación automática de la huella digital con los archivos de huellas almacenados.

  Después de una identificación válida, el usuario puede acceder a su PC, a la red o a un área restringida. El tiempo de verificación es de 3 - 4 segundos.

Figura 15. Reconocimiento por medio de la huella dactilar

- **Reconocimiento por medio de la mano**: El usuario ha de colocar la mano sobre una superficie de metal con cinco hendiduras que aseguran la correcta colocación de cada uno de los dedos o sobre la superficie de un scanner. El tiempo de verificación es de 2-3 segundos.

Figura 16. Reconocimiento por medio de la mano

- **Reconocimiento facial:** una cámara captura la imagen del usuario, y el sistema analiza ciertas características del rostro del individuo.

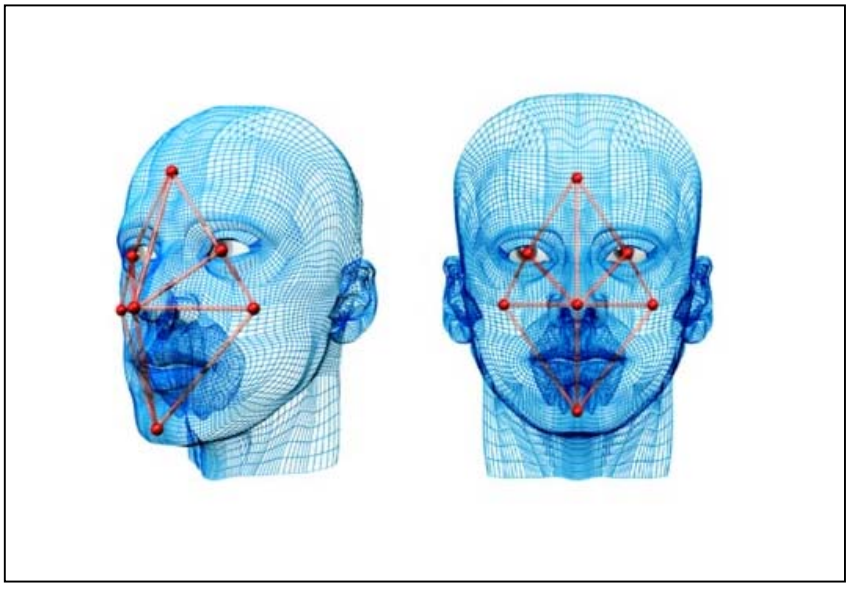


Figura 17. Reconocimiento facial

- **Reconocimiento por medio del iris**: El usuario se ha de posicionar cerca del dispositivo de verificación (periférico o cámara independiente). El

usuario ha de ubicar sus ojos en el dispositivo hasta que pueda ver el reflejo de sus ojos. La captura e identificación es casi inmediata. El tiempo de verificación es de 3-5 segundos.

Figura 18. Reconocimiento por medio del iris.

- **Reconocimiento por medio de la voz**: El usuario se ha de posicionar cerca del dispositivo de identificación (micrófono o teléfono) y ha de pronunciar la frase que ha utilizado para registrarse o bien repetir la frase dada por el sistema, siendo reconocido por el sistema a partir de las características de la voz grabada en el momento del acceso. El tiempo de verificación es de 4-6 segundos.

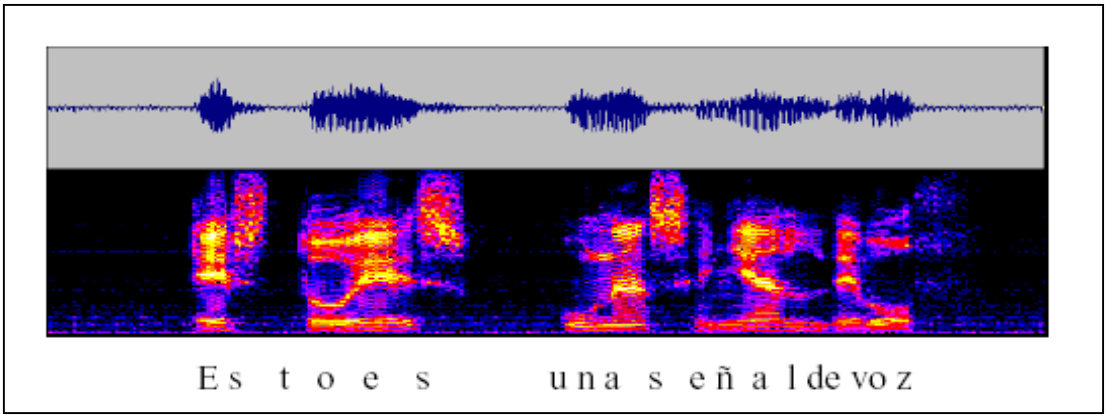


Figura 19. Reconocimiento por medio de la voz.

- **Reconocimiento por medio de la firma digital**: El usuario ha de firmar encima de la superficie de captura de la tabla. El tiempo de reconocimiento es de 2-3 segundos. Se utilizan digitalizadores que convierten las entradas escritas a mano en datos binarios. Algunos productos trabajan con digitalizadores basados en lapiceros. Pueden ser dispositivos externos (pequeños pads con estilos en forma de lapiceras), o computadores basados en lapiceras como PalmPilot.

Figura 20. Reconocimiento por medio de la firma digital.

- **Reconocimiento por medio del modo de escribir en un teclado:** El usuario ha de teclear su password o frase de acceso. El tiempo de verificación es de 2-3 segundos.

Figura 21. Reconocimiento por medio del modo de escribir en un teclado.

2.7 Etapas del registro biométrico

Los sistemas biométricos convierten los datos derivados de un comportamiento o de una característica física en patrones, que se utilizan para la identificación posterior.

Las etapas del registro biométrico están compuestas por múltiples procesos como son: la captura, el registro y la extracción de las características, las cuales se describen a continuación:

- **Captura**. Es el proceso a través del cual el usuario ofrece los datos físicos o de comportamiento al sistema biométrico. La captura puede consistir en mirar en la dirección de la cámara o bien colocar el dedo en la superficie del escáner. En función del sistema biométrico, el usuario deberá permanecer quieto unos segundos, o pronunciar una frase con el fin de ofrecer la muestra biométrica correcta.

- **Registro**. Es el proceso a través del cual se extrae la muestra o muestras para ser valoradas y almacenadas siguiendo el proceso del sistema biométrico. El registro tiene lugar tanto en sistemas con un usuario, como en sistemas de más de un usuario, y consiste en establecer una relación entre la muestra facilitada por el usuario y los datos de identificación almacenados (Ej. Nombre y C.I.). Si se presentan problemas en el registro, el usuario debe intentarlo de nuevo, ya que puede suceder que la captura (cantidad de datos de la muestra) no haya sido suficiente para crear la plantilla de registro.

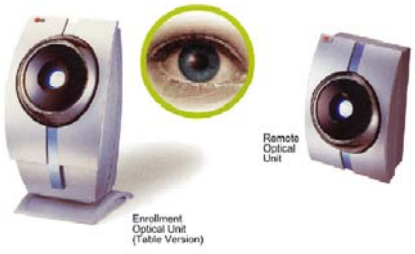
Es importante aclarar el concepto de muestra biométrica, la cual consiste en la característica física o de comportamiento captada durante la fase de captura que se utiliza para generar los patrones biométricos. También se denomina “información biométrica”. Los siguientes tipos de muestras están asociados a cada una de las tecnologías biométricas existentes, (ver tabla 1):

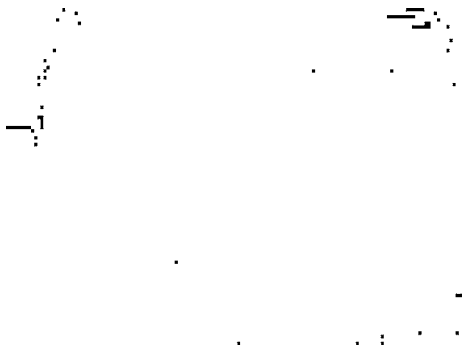
TECNOLOGÍAS BIOMÉTRICAS	TIPOS DE MUESTRAS
Reconocimiento de la huella dactilar	Imagen de la huella dactilar.
Reconocimiento de la mano	Imagen en 3D de la parte superior y laterales de la mano
Reconocimiento facial	Imagen de la cara
Lectura de la retina	Imagen de la retina
Lectura del iris	Imagen del iris
Reconocimiento de la voz	Grabación de la voz
Reconocimiento de la firma	Imagen de la firma y grabación de la dinámica de los movimientos
Reconocimiento de la forma de escribir en el teclado	Grabación de los caracteres utilizados y otras medidas relacionadas con la dinámica.

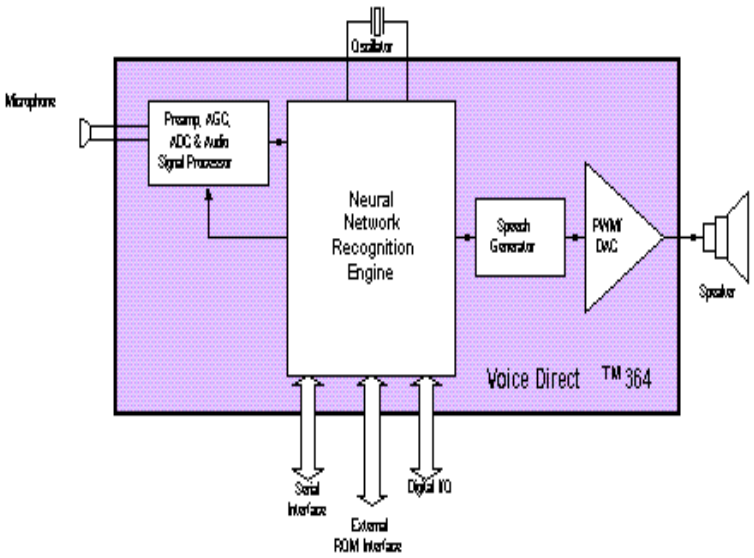
Tabla 1. Tipos de muestras asociados a las tecnologías biométricas.

Para realizar el registro biométrico es necesario contar con algún dispositivo de captura, que es el hardware utilizado para capturar las muestras biométricas. Los siguientes dispositivos de captura están asociados a cada una de las siguientes tecnologías biométricas:

TECNOLOGÍAS BIOMÉTRICAS	DISPOSITIVOS DE CAPTURA
Reconocimiento por medio de la huella dactilar	 Figura 22. Lector óptico integrado en un teclado (Keytronic de Identix).  Figura 23. Chip de silicio (Precise 100MC. de Precise Biometrics).  Figura 24. Lector por ultrasonido que contiene adicionalmente dispositivo para identificación de tarjetas magnéticas y claves numéricas opcional. Series 700 ID Station. (Fabricado por Ultra-Scan).

TECNOLOGÍAS BIOMÉTRICAS	DISPOSITIVOS DE CAPTURA
Reconocimiento por medio de la huella dactilar	 Figura 25. Lector óptico (Fingerscan V20 UA. Fabricado por Identix).
Reconocimiento facial	 Figura 26. Cámara integrada en el PC con software de reconocimiento facial (TrueFace Network).
Reconocimiento por medio del iris	 Figura 27. Cámara instalada en una estación central que almacena la información del usuario y cámara remota conectada en red a la estación central que captura los datos. Cámara de LG Electronics, Iris Access TM 3000.

TECNOLOGÍAS BIOMÉTRICAS	DISPOSITIVOS DE CAPTURA
Reconocimiento por medio de la retina	 Figura 28.Scanner de retina Icam 2001- EyeDentify
Reconocimiento por medio de la mano	 Figura 29. Lector biométrico basado en el reconocimiento tridimensional de la mano. Solución Biométrica Handkey II de Recognition Systems.

TECNOLOGÍAS BIOMÉTRICAS	DISPOSITIVOS DE CAPTURA
Reconocimiento por medio de la voz	 Figura 30. Chip de reconocimiento de voz para control de Sensory
Reconocimiento por medio de la firma	 Figura 31. Bolígrafo sensible al movimiento y lectora verificadora de firma de Biometricstore
Reconocimiento por medio de la forma de escribir en el teclado	 Figura 32. Teclado en el PC o en un terminal móvil

- **Extracción de las características**. Es el proceso automático de codificación y almacenamiento de las características distintivas de la muestra biométrica con el fin de generar la plantilla de registro. El proceso de extracción de características puede incluir varios grados de imagen o de muestras procesadas con el fin de obtener una cantidad suficiente de datos precisos. Por ejemplo, las tecnologías de reconocimiento de la voz pueden filtrar determinadas frecuencias y patrones así como las tecnologías de reconocimiento de la huella dactilar pueden comprimir los patrones presentes en la huella dactilar (lazo, arco y espiral) hasta el tamaño de un píxel. Además, si la muestra es inadecuada para formar la extracción de la característica, el sistema biométrico indicará al usuario que ofrezca otra muestra, a través de algún tipo de aviso de feedback. Por otra parte la forma en que el sistema biométrico extrae las características varía en función del fabricante. Las características más comunes que se utilizan en el proceso de extracción son las siguientes, (ver tabla 2):

TECNOLOGÍAS BIOMÉTRICAS	CARACTERÍSTICAS EXTRAÍDAS
Reconocimiento de la huella dactilar	Localización y dirección del comienzo y fin de los arcos y bifurcaciones de la huella dactilar
Reconocimiento de la voz	Frecuencia, cadencia y duración del patrón de voz
Reconocimiento de la cara	Posición relativa y forma de la nariz, posición de las mejillas
Reconocimiento del iris	Forma del iris
Reconocimiento de la retina	Forma de los capilares de la retina
Reconocimiento de la mano	Alto y ancho de los dedos y juntas entre los dedos y la mano
Reconocimiento de la firma	Rapidez, fuerza, presión y apariencia de la firma
Reconocimiento de la escritura en el teclado	Secuencia del tecleo, duración entre caracteres

Tabla 2. Características biométricas que se utilizan en el proceso de extracción

Luego del proceso de extracción de la característica, está es organizada y almacenada en forma de una plantilla. Una plantilla (template) son datos que se derivan de las características biométricas de un individuo, que se utiliza para obtener las correspondencias biométricas en el proceso de la comparación. La plantilla se crea a través de un proceso algorítmico que transforma las características diferenciales de la muestra en un número. Es decir, la plantilla es una representación numérica de la imagen de la muestra.

El concepto de plantilla es uno de los elementos que definen la tecnología biométrica a pesar de que no todos los sistemas biométricos utilizan plantillas para realizar el proceso de comparación. Existen sistemas de reconocimiento como la voz, que no utilizan plantillas sino la muestra original para realizar la comparación biométrica.

Las plantillas de registro se crean en la primera interacción del usuario con el sistema biométrico y se almacenan para ser utilizadas en futuras comparaciones. Se pueden utilizar múltiples muestras para generar una plantilla de registro. El reconocimiento facial, por ejemplo utiliza varias imágenes de la cara para generar esta plantilla.

Las plantillas de verificación se generan durante el proceso de verificación, al comparar la característica con la almacenada en la plantilla. La plantilla de verificación se deriva normalmente de una única muestra y la plantilla procedente de una única imagen facial se puede comparar con la plantilla de registro para determinar el grado de similitud.

2.8 Exactitud de los sistemas biométricos

Un factor importante en cada sistema de identificación biométrico son las tasas de falsas aceptaciones y falsos rechazos. Las primeras se refieren a reconocer

como correcto a la persona indebida, mientras que las segundas dan cuenta de los no reconocimientos de usuarios legítimos.

Uno de los aspectos más interesantes de la tecnología biométrica es que los patrones biométricos descritos se generan cada vez que el usuario interactúa con el sistema. Por ejemplo, el registro de dos muestras sucesivas de la misma huella dactilar en el dispositivo biométrico puede generar archivos totalmente diferentes. Estos archivos, cuando son procesados por el algoritmo del fabricante, son reconocidos como de la misma persona, aunque no sean idénticos. En teoría, un usuario puede colocar su dedo sobre el dispositivo biométrico varias veces y nunca generar datos idénticos.

Por lo tanto, para la mayoría de las tecnologías, no existe una correspondencia del 100%. Esto no implica que los sistemas no sean seguros y la mayoría de los sistemas biométricos son capaces de reconocer la identidad con un margen de error de menos del 1/100.000. Los sistemas biométricos deben elegir los archivos que le servirán para la identificación, y este proceso de decisión contiene varios pasos que se describen a continuación:

- **Correspondencia:** es la comparación de patrones biométricos para determinar el grado de similitud o correlación. Un intento de correspondencia tiene como resultado una puntuación que se compara con una medida predeterminada. Si el resultado es superior al umbral predeterminado por el sistema (threshold), el resultado es una correspondencia; si la puntuación está por debajo del umbral predeterminado por el sistema, el resultado es una no correspondencia.

  El proceso de correspondencia comprende la comparación entre patrones: el de verificación (creado a partir de la lectura de la muestra en un intento de acceso) con la plantilla de registro almacenado previamente. En los sistemas de verificación con un usuario, existe generalmente una única

plantilla de verificación que se compara con la plantilla de registro. En los sistemas de identificación de más de un usuario, la plantilla de identificación se puede comparar con docenas, decenas e incluso millones de archivos de registro.

- **Puntuación:** Es un número que indica el grado de similitud o correlación en la correspondencia biométrica. Los sistemas de autenticación tradicionales: (passwords, PINs, claves y tarjetas inteligentes) son binarios y ofrecen una respuesta de si/no. Este no es el caso de la mayoría de sistemas biométricos. Casi todos los sistemas biométricos están basados en algoritmos que generan una puntuación después de un intento de correspondencia. Esta puntuación representa el grado de correlación entre la plantilla de verificación y el de registro. No existe una escala estándar utilizada para la puntuación biométrica: para unos fabricantes se debe utilizar una escala 1 a 100, mientras que para otros se debe utilizar otra de 1:1; algunos fabricantes utilizan una escala logarítmica y otros una escala lineal. Independientemente de la escala utilizada, la puntuación de la verificación se compara con el nivel de umbral del sistema (threshold) para determinar el éxito de un intento de correlación. La mayoría de los sistemas devuelven una puntuación durante el registro, denominado puntuación de registro o puntuación de calidad. Esta puntuación representa el éxito en el proceso de extracción de las características distintivas de la muestra biométrica. Si la muestra es rica en información, es probable que exista una puntuación alta de registro. Esta puntuación no se utiliza en el proceso de correlación, pero se puede utilizar para determinar si un usuario puede registrarse con éxito. Una puntuación baja puede indicar que el usuario no pudo ser verificado de forma confiable.

- **Umbral de seguridad (Threshold):** Es un número predefinido, frecuentemente controlado por el administrador del sistema biométrico, que establece el grado de correlación necesario para que la correspondencia dé

como resultado una coincidencia de patrones. Si la puntuación resultante de una comparación de patrones supera este umbral predeterminado, se considera que la plantilla coincide (a pesar de que las plantillas en sí mismos no sean idénticas). El umbral (threshold) para el éxito de una verificación, será más permisivo en sistemas de baja seguridad que en sistemas de alta seguridad.

- **Decisión**: es el resultado de la comparación entre la puntuación y el nivel de seguridad predeterminado por el sistema. Las decisiones que puede realizar el sistema biométrico incluyen: correlación, no-correlación y no concluyente, a pesar de que puedan existir varios grados de fuerte correlación y no correlación.

  Dependiendo del tipo de sistema biométrico empleado, una correlación positiva puede garantizar el acceso al sistema, una no correlación puede limitar el acceso, mientras que el resultado indeterminado significa que el usuario ha de reintentar.

2.9 Biometría: la nueva dimensión en la seguridad para empresas

La biometría es utilizada por las empresas para reforzar el nivel de seguridad en la autenticación de usuarios en el acceso a PCs, redes, archivos o lugares. La seguridad biométrica es la tecnología por medio de la cual se autentica un individuo en sistemas biométricos y no se realiza mediante claves simétricas, públicas o privadas (PKI), sino por lo que es en sí el individuo: huellas dactilares, análisis facial, análisis de iris, reconocimiento de voz, etc.

La seguridad biométrica es uno de los métodos para controlar el acceso a la información o a los sitios. Un dispositivo biométrico autentica la identidad de un usuario a través de sus rasgos físicos, como la huella dactilar o el iris, para asegurar que la persona que accede a máquinas y recursos restringidos, es la que

verdaderamente está autorizada para hacerlo. De esta manera, la seguridad biométrica refuerza el punto débil de muchos sistemas de seguridad informáticos. Es decir, verifica la identidad real del usuario, no a través de privilegios mediante objetos (como tarjetas inteligentes) ni de conocimientos (como un PIN o una contraseña), ambos transferibles entre las personas.

Frente a los requisitos de las empresas que manejan información confidencial, la biometría ofrece una amplia gama de aplicaciones para la protección de datos y entornos restringidos:

- El control de acceso a máquinas y redes mediante la verificación por un rasgo físico.
- La protección de máquinas, a través de dispositivos que requieren autenticación biométrica (Mouse biométrico).
- La protección de espacios físicos, donde sólo pueda entrar personal autorizado.
- El acceso online a servicios y cuentas privadas mediante la autenticación biométrica para aumentar la seguridad en los servicios remotos.

2.10 Aspectos a ponderar en la adquisición y selección de un sistema biométrico

En función de la situación en que se necesite realizar autenticación segura del usuario, es esencial determinar cuál es la técnica biométrica (ó combinación de técnicas de autenticación) más adecuada. Entre los aspectos que se deben ponderar para decidir cuál sistema biométrico es más conveniente, se encuentran los mencionados a continuación:

- Necesidad de adquirir un dispositivo con tecnología biométrica (lector de huella dactilar, micrófono, cámara, etc.) para controlar accesos.
- Variabilidad en el tiempo de la plantilla a identificar (afonías ó catarros en voz, uso de lentes/bigote/barba/etc. en rostro, etc.).

- Probabilidad de error individual de cada una de las técnicas (entre uno por cien y uno entre varios millones, en función de la técnica elegida).
- Aceptación por parte del usuario de las técnicas, en función de si son o no intrusivas o peligrosas, cómodas, que mantengan la privacidad, sencillas de usar, etc.

2.11 Limitaciones de las técnicas biométricas para el control de acceso

A pesar de presentar la tecnología biométrica como una panacea al problema de claves inseguras o de pérdida o duplicación de elementos físicos de seguridad, esta tecnología presenta problemas a la hora de afrontar situaciones atípicas. ¿Qué ocurre, por ejemplo, sí:

- El usuario sufre una amputación del dedo o daños físicos?
- El usuario sufre de ceguera parcial o no puede pasar el escáner retiniano debido a enfermedades como catarata.
- El usuario tiene ronquera y la voz es irreconocible (si esta afónico o tiene congestión nasal)?

Estas situaciones se pueden considerar atípicas, pero los sistemas biométricos deben diseñarse para hacerles frente. En todo caso los fabricantes deben dar garantía de que en situaciones así lo peor que puede ocurrir es que se le niegue el acceso a un usuario legítimo.

Por otra parte muchas pruebas de campo recientes demuestran que, incluso ante situaciones muy favorables, resulta trivial, en la mayoría de los casos, provocar falsos positivos en los sistemas biométricos evaluados, es decir, que un atacante puede burlar la verificación de estos sistemas.

CAPITULO III

LA AUTENTICACIÓN CON LOS SISTEMAS BIOMÉTRICOS

3.1 Métodos de autenticación

Para acceder a un sistema se sigue un proceso de dos pasos: primero, el usuario dice al sistema quién es (identificación), y segundo, el sistema comprueba que el usuario es efectivamente quién dice ser (verificación). La dificultad está en el segundo paso, pues los sistemas de información tradicionales no disponen de mecanismos sensoriales ni cognitivos, y sólo pueden reconocer al usuario mediante una clave que lo distinga del resto de las personas. Las claves que se utilizan en este proceso de autenticación se suelen dividir en tres grupos: claves informativas, claves físicas y claves biométricas. A continuación describiremos cada uno de ellas (White, 1996).

Claves informativas:

El sistema comprueba la identidad del usuario solicitando y obteniendo información que únicamente este último conoce. Esta información puede ser una palabra o frase clave, que en unos casos elige el propio usuario y en otros es asignada por el sistema, y se denomina contraseña. Pero también puede ser la respuesta a un cuestionario que el sistema conforma y realiza en cada ocasión basándose en datos recopilados previamente y que son específicos del usuario.

La efectividad de las claves informativas reside en que ese conocimiento siga siendo compartido exclusivamente por el sistema y el usuario, manteniéndose secreto para el resto del mundo. Para ello es necesario que la información no pueda ser sustraída ni adivinada.

Claves físicas:

El sistema comprueba la identidad del usuario solicitando e identificando un objeto que únicamente este último posee. Este objeto debe ser reconocible por algún periférico del computador, por lo que suelen utilizarse dispositivos de formato estándar en los que el elemento diferenciador no es visible. Así, las claves físicas más comunes son las tarjetas magnéticas, idénticas en formato a las tarjetas de crédito, que poseen una banda magnética donde se graban datos sobre la tarjeta y su dueño siguiendo un estándar internacional. Las tarjetas inteligentes mantienen el tamaño estándar de las tarjetas de crédito, pero llevan un circuito integrado que, además de guardar información sobre el usuario de la tarjeta, es capaz de realizar pequeñas operaciones con esos datos. Por ejemplo, estas tarjetas pueden estar programadas para aplicar su propio sistema de cifrado de los datos, para validar su integridad o para verificar la autenticidad de la propia tarjeta.

La efectividad de las claves físicas se basa en que el usuario conserve permanentemente la posesión del dispositivo que le acredita como tal, pero también en que dicho dispositivo no pueda ser falsificado.

Claves biométricas:

El sistema biométrico comprueba la identidad del usuario solicitando y contrastando un dato biométrico específico de este último. Como claves biométricas más comunes se utilizan características físicas (como las huellas dactilares, el mapa retinal, los rasgos faciales, la geometría de las manos, el olor corporal, las marcas del iris, etc.) y habilidades (como la firma, la frecuencia de tecleado y la voz). Para poder utilizar claves biométricas para autenticar a las usuarias son imprescindibles dos requisitos, uno de hardware y otro de software. En primer lugar el sistema debe disponer de un periférico adecuado (sensor) para leer el dato biométrico que se le suministra. Pero no es menos importante disponer de un mecanismo de comparación entre el patrón capturado por el dispositivo y lo almacenado en el sistema, para lo

cual es imprescindible disponer de un sistema de representación del dato biométrico en cuestión que permita estas manipulaciones con confiabilidad.

La efectividad de las claves biométricas se fundamenta en que el sistema de reconocimiento sea lo suficientemente preciso como para distinguir sin duda posible, unas personas de otras, y al mismo tiempo lo suficientemente flexible como para admitir las variaciones puntuales que los datos biométricos de cada persona experimentan con el tiempo. También es importante que los sensores sean capaces de detectar los intentos de falsificación.

Los distintos tipos de claves de autenticación no son excluyentes entre sí. Por ejemplo, es muy frecuente la combinación de tarjetas magnéticas con contraseñas, que pueden estar almacenadas en el sistema o en la propia tarjeta. Asimismo, muchas veces se utilizan claves de autenticación para acceder no al sistema, sino a su entorno (edificios, sala de servidores), por lo que resuelven problemas propios de seguridad física.

3.2 Tipos de mediciones en los sistemas biométricos

Hay una distinción importante entre los medios tradicionales de la autenticación (tales como contraseñas, cuestionarios) y la biometría. Una contraseña (o un PIN) cuando es introducido por un usuario puede que sea correcto o incorrecto, así que al usuario puede que sea aceptado o rechazado.

Los sistemas biométricos pueden mostrar variaciones al momento de medir características o comportamiento humano. Las variaciones de medidas que se registran en estos sistemas, las cuales en lenguaje técnico se conocen como error Tipo I (error de falso rechazo) y error Tipo II (error de falsa aceptación). El ajuste de la tolerancia del error es crítico para el funcionamiento del sistema. El falso rechazo (false rejection, FR) causa la frustración y la falsa aceptación (false acceptance, FA) causa problemas de seguridad. Los errores Tipo I y Tipo II pueden ser graficados en

curvas de porcentajes de error de falso rechazo (false rejection rate, FRR) y de falsa aceptación (false acceptance rate, FAR), ver figura 32, las cuales se relacionan con el ajuste del umbral de la sensibilidad del sistema. Idealmente estas curvas deberían ser iguales a cero, pero en la realidad estas curvas se cruzan sobre un punto del umbral (equal error rate, EER) en el cual los errores de FR y FA son iguales. Mientras más bajo es este punto, más exacto es el dispositivo. Un ajuste del umbral reducirá el potencial para los errores FA, pero aumentaría los errores FR.

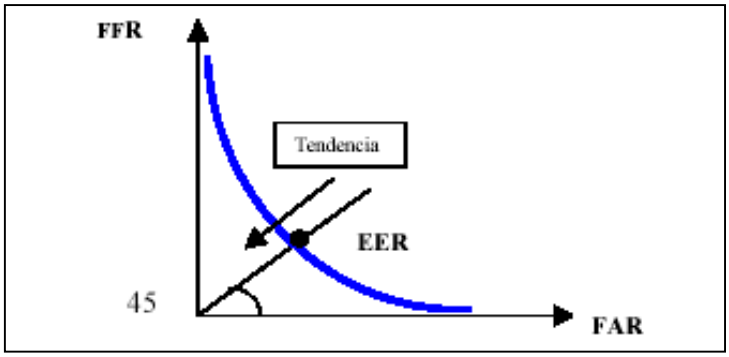


Figura 33.Relación entre FAR, FRR y ERR

Todos los sistemas deben tener la posibilidad de reajustar el umbral, para así poder aumentar o disminuir el nivel de la seguridad según sea necesario. La aceptación del usuario se debe también considerar para fijar el umbral. Por lo tanto el uso dictará cual será el mejor ajuste. Se está intentando establecer estándares para asegurar que se utilicen los mismos criterios y así obtener las medidas exactas de la tasa-error. Puesto que el nivel de tolerancia es ajustable, hay una compensación entre los dos errores. Algunos fabricantes biométricos se aprovechan de esto y presentan solamente el mejor de los dos errores.

3.3 Plantillas

Por una plantilla definimos la medida biométrica registrada de un usuario. Una plantilla se asocia a un identificador, para ser requerido cuando se solicita. El almacenaje de las plantillas de los usuarios depende del tipo de uso que se le dé al

dispositivo biométrico y del tamaño de las plantillas y se pueden almacenar en la memoria del dispositivo biométrico, en una base de datos central, o en tarjetas de plástico.

3.3.1 Memoria del dispositivo biométrico

Las plantillas se pueden almacenar en la memoria del dispositivo biométrico y su capacidad de almacenamiento varía según el dispositivo que se utilice. Almacenar las plantillas en la memoria del dispositivo aumenta su seguridad puesto que las plantillas no se transmiten. Es también económico puesto que no se requiere ningún costo adicional en tarjetas para los usuarios. Sin embargo ésta no es la mejor opción si su uso es masivo (Ej.: base de datos de criminales) o si los usuarios necesitan ser verificados en diversas localidades (Ej.: agencias bancarias, aeropuertos, oficinas de seguridad social, etc.).

3.3.2 Base de datos central

Las plantillas se pueden almacenar en una base de datos central si el número de los usuarios es grande o la verificación remota es necesaria. El aspecto de la seguridad de almacenar plantillas en una base de datos central debe ser considerado cuidadosamente. La seguridad de las plantillas se puede comprometer debido a:

- El uso erróneo o el abuso de la base de datos por administradores o intrusos internos.
- Transmisión insegura a los dispositivos biométricos remotos.
- Sistemas y redes de comunicación vulnerables.
- Abuso de privilegios
- Protocolos de comunicación y algoritmos vulnerables.

Antes de transmitir plantillas sobre Internet, se debe aumentar su seguridad. Una red pública en sí misma no es segura, debido a que las plantillas transmitidas sobre esta red pueden ser interceptadas por algún intruso o por administradores o

empleados de la red. Posibles soluciones a este problema son el uso de líneas dedicadas o de VPN (Virtual Private Network). Otra alternativa puede ser el establecimiento de un TTP (Trusted Third Party) o de una red de TTPs que aseguran la transmisión y el almacenaje seguro de las plantillas y que proporciona la seguridad apropiada de la base de datos. Si los algoritmos implicados en la transmisión son vulnerables a un ataque criptográfico las plantillas pueden ser reveladas. Si los protocolos de comunicación son débiles, entonces la seguridad de las plantillas está en riesgo.

3.3.3 Tarjetas inteligentes

Este método de almacenaje permite a usuarios llevar con ellos sus plantillas de identificación. Este método es el más apropiado cuando:

- El número de usuarios es muy grande como para ser almacenado en una base de datos central.
- Existe la necesidad de los usuarios de ser verificados remotamente.
- Existe la necesidad de que las plantillas sean verificadas rápidamente.
- La sensibilidad y la seguridad de la transmisión es una prioridad.

3.4 Amenazas

Las amenazas son consideradas como violaciones potenciales de la seguridad con resultados perjudiciales. Estos pueden ser previstos o inesperados, y existen debido a una vulnerabilidad en el sistema. Si un usuario no autorizado invade un sistema, él puede dañar o destruir la información, los sistemas operativos y los programas, divulgar la información o causar interrupciones (daños en el sistema, redes, organizaciones, instituciones).

Las fuentes de amenazas son las siguientes:

- *Físicas*: incluyen los desastres naturales (incendio, tormenta, daños por agua entre otros) y las condiciones ambientales (polvo, humedad, etc.).

- *Técnicas*: son producto del equipo de un sistema (hardware) o del software que pudo no haber realizado su función (falla), o puede ser que la realice de una manera inapropiada (malfuncionamiento).
- *Humanas*: que es la fuente principal de las fugas de la información. Incluye a los usuarios no autorizados que desean dañar un sistema, y a usuarios autorizados que emplean mal el sistema ya sea deliberadamente o accidentalmente. Las amenazas humanas se pueden categorizar más a fondo en internas y externas. Las amenazas internas son: empleados disgustados, hackers, antiguos empleados, administradores del sistema, administradores de la LAN y de la base de datos, entre otros. Las amenazas humanas externas se presentan como la forma de espionaje comercial, industrial, militar, fabricantes, etc.
- *Teóricas:* incluyen vulnerabilidad de los algoritmos, de los protocolos y de las herramientas matemáticas usadas para la ejecución del sistema biométrico.

Las amenazas que pueden ser identificadas son:

- Intrusión
- Negación del servicio
- Acceso a la información
- Corrupción de la información
- Uso no autorizado de los recursos
- Uso erróneo de los recursos
- Flujo de Información no autorizado.

3.5 Criterios para la selección de las tecnologías biométricas

La confiabilidad y la aceptación de las tecnologías biométricas dependen de la eficacia del sistema, de cómo éste se protege contra modificaciones y del uso no autorizado, de cómo los sistemas proporcionan soluciones a las amenazas (descritas

en la sección 3.4), de su capacidad y eficacia en autenticar e identificar a los usuarios.

La selección de los sistemas biométricos se basa en la puesta en práctica de cuatro pasos básicos:

- La captura de las características biométricas de los usuarios.
- La generación de la plantilla con los atributos de los usuarios.
- La comparación entre los datos de entrada contra la plantilla almacenada del usuario autorizado.
- La toma de decisión para aceptar o rechazar el acceso.

Antes de seleccionar los sistemas biométricos, es necesario evaluar los métodos biométricos de identificación en que estos están basados, los cuales utilizan: algoritmos, códigos fuentes, base de datos para almacenar plantillas, protocolos, claves y, si las plantillas son transmitidas, redes y sistemas de distribución. En muchos ambientes (militar y gubernamental) donde la solidez de la seguridad es muy importante, un sistema biométrico no será aceptado si no es seguro, por lo tanto se deben fijar los siguientes criterios para evaluar estas herramientas (Polemi, 1997):

1. Algoritmos correctos

   Los algoritmos empleados en biometría son similares, pero difieren en la tecnología usada para ponerlos en ejecución, tales como:

   - Métodos basados en modelos estadísticos
   - Programación dinámica
   - Redes neurales (neural networks).

2. Algoritmos seguros

   - Los algoritmos que son fáciles de descifrar ponen cualquier arquitectura de seguridad en riesgo, aunque esté muy bien construida.

Diversos algoritmos criptográficos ofrecen diferentes grados de seguridad, que son evaluados de acuerdo a cuan difícil pueden ser vulnerados. Por otro lado mientras más difícil sea vulnerarlo, mayor será su costo. Los sistemas biométricos que son utilizados en transacciones financieras donde está implicada mucha cantidad de dinero, los hace propensos de ser atacados, por lo que los algoritmos criptográficos deben ser los mejores y probablemente los más costosos, para así evitar que algún intruso pueda descriptarlo.

3. Buena selección de las claves: La selección de las claves es importante y deben ser elegidas bajo ciertas restricciones, de forma que el usuario no escoja alguna clave vulnerable. (Ej.: Utilizar frases suficientemente largas para que posteriormente sean convertidas en claves por medio de un algoritmo o usar cadenas de bits creadas por medio de algún proceso automático).

4. Códigos fuentes

- Los algoritmos criptográficos usados en los códigos fuentes deben ser seguros.

5. Base de datos seguras.

- El administrador de la base de datos debe ser personal de confianza.
- La plantilla que se encuentra en la base de datos debe ser almacenada, distribuida y manejada con altos niveles de seguridad.

6. Protocolos seguros

- Los algoritmos criptográficos usados en los protocolos deben ser seguros.
- Las técnicas criptográficas usadas para poner los protocolos en ejecución deben ser seguras.

- No se deberían encontrar defectos en los protocolos.

Las técnicas criptográficas usadas para poner en práctica los protocolos pueden ser vulnerables a los ataques. Algunos algoritmos se presentan solamente como que cumplen las normas ISO (International Organization for Standardization) y no se comprueba su vulnerabilidad. Por lo tanto, los criterios que se deben fijar para la evaluación apropiada de los métodos biométricos deben tomar en cuenta estas preocupaciones teóricas.

7. Redes y sistemas de distribución seguros.

Si las plantillas son transmitidas sobre una red, la seguridad de la red debe ser evaluada.

Los métodos biométricos necesitan ser evaluados por especialistas en evaluación de sistemas de seguridad. Algunas de las instituciones que se han especializados en esta área son: La NSA (National Security Agency), la compañía RSA Data Security Inc, El Instituto de Tecnología Federal en Suiza, La Universidad Tecnología de Queensland (Centro de Investigación de la Seguridad de la Información), La Universidad de Belgrado (Escuela de la Ingeniería Eléctrica), La Universidad de Kentucky (Departamento de la Ciencia de la Computación), La Universidad Occidental de Ontario, Canadá (Departamento de Informática), La Universidad de Technion, Israel (Departamento de Informática), La compañía HTL Brugg-Windisch, La compañía GRETAG Ltd, La Universidad Meridional de Luisiana (Centro de Estudios Avanzados por Computadora), La Universidad de Londres (Departamento de Informática), Universidad de Louvain (Departamento de Electricidad y Electrónica), La Universidad de Wincosin (Departamento de Computación).

La confiabilidad y la aceptación de un dispositivo biométrico dependen de sus características operacionales, técnicas, financieras y de fabricación, las cuales fijan

los criterios de selección de estos dispositivos como se describe a continuación (Polemi, 1997):

Operacional:

Los dispositivos deben ser *convenientes* para utilizar. Por ejemplo, el tiempo requerido para realizar funciones tales como registro del usuario, autenticación y verificación deben ser mínimos. En una cola del supermercado o en la entrada de una compañía en las horas laborables, (Ej.: de 8 a.m. a 5 p.m.) donde la verificación será realizada, el tiempo que se requiere para tomar la verificación es un criterio importante para elegir un dispositivo biométrico.

Otro factor importante en las tecnologías biométricas es la *aceptabilidad pública.* En actividades bancarias, la aceptabilidad del público es una prioridad para elegir un sistema biométrico puesto que los clientes pueden elegir otro banco (Ej.: los sistemas de la verificación del patrón de ojo no son muy aceptados). Un *uso amigable* es importante para que el dispositivo sea aceptado por el público. Un dispositivo de fácil utilización es conveniente, pero debe satisfacer las necesidades de seguridad del usuario, y estar acorde con los estándares sociales contemporáneos. Se encontró, por ejemplo, que a los japoneses no les gusta colocar la palma de su mano donde ya lo ha hecho otra persona. El dispositivo no debe ser *socialmente desagradable,* por ejemplo tener que quitarse los lentes de contacto en un lugar público y mirar por un dispositivo que inspira miedo, no será aceptado.

Un dispositivo es aceptado por el público si es *no discriminatorio* y factores humanos como: género, edad, profesión, condición física y psicológica de una persona no deben influenciar el funcionamiento del dispositivo biométrico. Las personas con problemas en la garganta o que esté afectado por una anestesia dental, pueden tener dificultades en ser verificadas por sistemas de autenticación de la voz.

Otros criterios operacionales son: la *unicidad* y la *exclusividad*. El resultado del proceso de la autenticación debe ser único, no debe cambiar cada vez que el dispositivo biométrico verifique al usuario y ninguna otra forma de identificación debería ser necesaria.

Técnicos:

Todos los componentes técnicos del dispositivo biométrico contribuyen en el tiempo de la autenticación. El *tiempo* requerido para medir las características humanas, crear las plantillas y almacenarlas debe ser mínimo. El ajuste de la *tasa de tolerancia* es importante para el funcionamiento de estos sistemas. Ambos errores deben ser cotizados explícitamente y ambos necesitan ser tan bajos como sea posible. Algunos fabricantes cotizan solamente el menor error, pero éste es engañoso. Los dispositivos deben ser *simples* para utilizar, *rápidos* y *exactos.*

Los dispositivos deben poder utilizarse bien, independientemente *de las condiciones ambientales* (luz, ruido, calor, humedad, humo, polvo, etc.). Por ejemplo, la mayoría de los lectores de la mano no pueden ser utilizados bajo altas o muy bajas temperaturas y solamente pueden ser usados en ambientes de interior controlados.

Deben ser *flexibles* en el ajuste del umbral, ya que el nivel de seguridad dependerá de para que será su uso.

Financieros:

El costo es un factor importante para elegir un dispositivo biométrico. Bajo el término “financiero” se tienen costos de equipos, de instalación y de entrenamiento. La mayoría de los dispositivos son costosos y esto es una barrera en la difusión del mercado biométrico.

La actualización de las plantillas puede ser un proceso costoso. Después de que las plantillas han sido creadas es complejo clasificarlas (en la base de datos

central se debería "particionar" el disco duro de manera que la búsqueda sea más rápida, en esas particiones se guardan las plantillas según una clasificación previa). Por otro lado existen dispositivos que pueden funcionar solo en ambientes controlados (donde debe haber una temperatura constante de 15-25°C). Adicionalmente debe ser considerado el costo del software utilizado por estos dispositivos, así como la administración del sistema biométrico.

Fabricación:

El sistema biométrico elegido debe estar soportado por diferentes fabricantes. Por otro lado éstos deben estar en capacidad de apoyar la puesta en marcha del sistema.

En conclusión diversos criterios deberán ser considerados de acuerdo al uso. Por ejemplo, si el presupuesto potencial de una compañía es grande, el costo no debería ser considerado como un factor clave para elegir un sistema biométrico, en cambio si la empresa tiene un presupuesto limitado y desea solucionar su problema de seguridad, entonces esta opción probablemente tendrá más peso a la hora de seleccionar el sistema (en el anexo 2 se encuentra un resumen de los criterios para la selección de tecnologías biométricas).

3.6 Estandardización de las pruebas

Las tecnologías de información deben ser internacionales en su alcance. Los métodos que se utilizan en Europa también deberían poder funcionar en EE.UU. y viceversa. Por lo tanto la estandardización es una condición importante para elegir. Puesto que las tecnologías biométricas son relativamente nuevas, no existen estándares publicados hasta la fecha. Sin embargo hay varios comités, asociaciones y organizaciones que se han formado para crear ciertos estándares. En el mercado existe una gran necesidad para que se creen y así lograr que los sistemas biométricos consigan ser explotados con éxito.

CAPITULO IV

ANÁLISIS Y DISCUSIÓN DE LOS SISTEMAS BIOMÉTRICOS

En este capítulo se describe cada sistema biométrico por separado con el objeto de examinar su efectividad. En detalle se examinará cómo responden a algunas de las amenazas y a los criterios descritos en el capitulo anterior. Desafortunadamente no tenemos un método exacto para la evaluación completa de las tecnologías biométricas, además la prueba de estos sistemas implica tener a disposición laboratorios especiales, equipos para las pruebas y personal entrenado. Por lo tanto, realizaremos un análisis de las tecnologías biométricas basados en la literatura disponible, tal como informes, reportes técnicos, estudios, manuales y en los resultados obtenidos del experimento realizado para engañar un mouse biométrico.

Se comentará sobre los sistemas biométricos disponibles y en desarrollo, así como las compañías proveedoras. Para cada método biométrico se mostrará las áreas en que pueden ser utilizadas.

4.1 Técnicas biométricas fisiológicas

Las tecnologías orientadas a la identificación biométrica pretenden abordar la problemática de identificar de forma automática a una persona a través de algunos de sus rasgos personales. Estos rasgos pueden ser directamente observados a partir de características fisiológicas, como sucede en el caso de las huellas dactilares, la cara, el iris, la retina y la geometría de la mano. A continuación se analizan cada una de las técnicas biométricas fisiológicas:

4.1.1 Verificación de la huella dactilar

Como ya se ha dicho, los patrones de las huellas dactilares son diferentes para cada individuo y no presentan cambios cuando el cuerpo crece. La clasificación

de huellas dactilares se basa en ciertas características (arco, lazo y espiral). Los sistemas disponibles para reconocer estas características son complejos, algunos no son capaces de distinguir una huella dactilar de un usuario real de la huella dactilar copiada. Una cirugía en el dedo, alguna lesión o ciertas condiciones de manos puede afectar el funcionamiento de los sistemas. El método tiene también el problema de la aceptación del público o de los usuarios.

Los sistemas de la huella dactilar se pueden utilizar en diferentes aplicaciones: En su aplicación legal, las huellas dactilares se comparan (generalmente manualmente) contra una base grande de huellas digitales. El FBI desarrolla una red de datos digitales en el ámbito nacional para determinar una identificación y emparejarla con los expedientes anteriores. Esta red proporcionará un acceso rápido al nuevo sistema automatizado integrado de identificación de huella digital AFIS (Automated Fingerprint Identification System) y acelerará la identificación de algún sospechoso. Asimismo el FBI para comprimir su base de datos de huellas dactilares utiliza la aplicación *wavelets* que comprime imágenes digitales.

Los EE.UU. también están desarrollando una red con las huellas digitales de los niños para su posterior identificación (para los casos en que la identidad pudo haber sido cambiada), comparando las huellas dactilares contra una base de datos nacional de las huellas digitales de los niños.

Efectividad

Operacional:

Muchas personas asocian la verificación de la huella dactilar con criminales. En actividades bancarias su uso es aceptado si se utiliza para prevenir fraude con tarjetas de crédito. Esto se desprende de una investigación presentada en el foro *"Prevención del fraude con dinero plástico"* en el Reino Unido (1995). En esta investigación se pidió la opinión de los usuarios con respecto a las siguientes tecnologías: PIN, firma y huella dactilar. El resultado fue que los sistemas de

reconocimiento a través de huella dactilar eran preferidos como muy seguro, rápido, confiable y fácil de utilizar.

Los sistemas de la huella dactilar por supuesto no se pueden utilizar en personas a los que le falten las manos o dedos. Las personas con los dedos dañados o hinchados pueden tener problemas al ser verificado por estos sistemas. En los entornos de trabajo, donde los trabajadores necesitan usar los guantes (Ej.: plantas de energía, laboratorios médicos o químicos, etc.) este método de identificación no será apropiado. La edad, el género, la ocupación, la raza y los factores ambientales influyen en la validez de los sistemas de la huella dactilar.

Técnica:

Las huellas dactilares y las impresiones de la palma son extremadamente exactas puesto que confían en cualidades físicas inmodificables, pero para el uso como control del acceso se requiere dispositivos de entrada especiales. Por otra parte estos dispositivos no son siempre compatibles con los estándares de telecomunicaciones, por lo tanto no son recomendables cuando la base de datos central se encuentre en una oficina remota.

Un sistema de huella dactilar puede trabajar con sistemas de tarjetas, tales como tarjetas inteligentes y tarjetas ópticas, para verificación de la identidad. Estas tarjetas son de gran seguridad y pueden ser usadas para programas de asistencia social, cedulas de identidad, licencias de conducir, pasaportes, tarjetas de crédito, etc. En el informe de la GAO (General Accounting Office "Electronic Benefits Transfer, Use of Biometrics to Deter Fraud in the Nationwide EBT program", USA, 1995) dice que la "huella dactilar puede ser la opción más viable" entre los métodos biométricos investigados: verificación de la voz, geometría de la mano, verificación de la firma y exploración de la retina. El proyecto de la CASCADE (Chip Architecture for Smart Cards and Secure Portable Devices, Esprit Project EP8670, Data Sheet

1995) afirma que las huellas dactilares son la mejor tecnología para reducir los tiempos de autorización en las aduanas.

Aplicación en la actualidad:

- Industria médica y de seguro.
- Actividades bancarias
- Agencias estadales
- Seguridad de la información
- Autenticación de identidad
- Cuerpo de policía
- Plantas eléctricas o de energía
- Servicios de inmigración
- Seguridad en aeropuertos
- Seguro social
- Identificación de niños extraviados
- Sistema de base de datos
- Acceso para computadoras
- Acceso a sistemas informáticos
- Control de acceso físico

Algunos productos comerciales:

- WinFing 3.1 (PrintScan Internacional, U.S.A.)
- Explorador De la Huella digital (The National Registry, U.S.A.)
- FingerCheck (Startek, Taiwan)
- FingerScanner (FingerMAtrix, U.S.A.)
- FingerScan (Australia)
- TouchPrint 600 (Identix, U.S.A.)

4.1.2 Verificación del iris y retina

Los oftalmólogos propusieron originalmente que el diafragma del ojo podía ser usado como una clase de huella digital óptica para la identificación personal. Su proposición se basaba en resultados clínicos, donde se demostraba a través de fotografías clínicas, que cada iris es único y permanece sin cambios.

Las características del iris que realzan la conveniencia para su utilización en un sistema de identificación automática son:

- El iris esta protegido contra el ambiente externo.
- La imposibilidad de modificarse quirúrgicamente el iris sin que haya riesgo de perder la visión.
- La respuesta fisiológica del iris a la luz, lo que proporciona una prueba natural fehaciente de que no es un artificio.
- La facilidad de capturar su imagen a cierta distancia del usuario sin que haya contacto físico.

En un estudio científico de la IEEE (Daugman, 1993) se prueba matemáticamente que existen diferencias en las características del iris entre individuos para concluir que el iris tiene la misma singularidad que una huella dactilar convencional. También se han desarrollado algoritmos que permiten extraer una descripción detallada y confiablemente del iris de una imagen de video en vivo y generar un código compacto que permita tomar una decisión sobre la identidad del individuo con una alta confianza estadística.

Efectividad

Aceptación pública:

Los sistemas de reconocimiento del iris en muchas áreas de aplicación tienen problemas de aceptabilidad por parte del publico. Por ejemplo, en el proyecto INFOSEC Health Sign (1994), a usuarios en el Reino Unido, Grecia e Italia se le presentaron diferentes opciones tecnológicas para uso como interfaz electrónica de acceso en los sistemas de información del hospital. Las opciones incluyeron explorador de la retina, identificación de la huella dactilar, sistemas del análisis de la voz y la firma manuscrita. El resultado de la encuesta fue que en el Reino Unido los exploradores retinianos eran los menos aceptables y en Italia fue totalmente inaceptable.

Los sistemas de reconocimiento del iris tenían problemas publicos de aceptabilidad en el pasado debido al uso de un rayo de luz infrarroja. Los reciente sistemas registran la imagen del iris fácilmente a cierta distancia del usuario, pero las personas siguen escépticas de esta tecnología. Personas ciegas o con daños severos en los ojos (diabéticos) no pueden utilizar este método biométrico.

Técnica:

Los vasos sanguíneos retinianos caracterizan ampliamente al individuo, así que la exactitud es una de las ventajas de este método de identificación. Los ojos artificiales duplicados son inútiles puesto que no responden a la luz. Reciente investigaciones médicas ha demostrado que los patrones retinianos no son tan estables como se pensaba y presentan variaciones críticas cuando hay una disfunción o una enfermedad del órgano (Marsh, 1996).

Aplicación en la actualidad:

- Acceso de alta seguridad para servicios del gobierno o financieros
- Instalaciones correccionales

Algunos productos comerciales:

- IrisScan 2020, System 2000 EAC (IrisScan, U.S.A.)
- IrisIdent System (Sensor, U.S.A.)
- 2001 (Eye Dentify, U.S.A.)

4.1.3 Reconocimiento facial

La premisa de este método esta en que las características de la cara (el tamaño de la nariz, la forma de los ojos, la barbilla, las cejas, la boca) son únicas para cada individuo. Este método ahora esta siendo ampliamente desarrollado, utilizando para ello costosos procesos de redes neurales. Para ello se utilizan cámaras fotográficas que extraen datos de las características faciales y se

almacenan en una tarjeta inteligente o una tarjeta magnética. La persona presenta su tarjeta mientras una pequeña cámara fotográfica le toma una imagen. El software compara los datos de la persona con los datos almacenados en la tarjeta.

Efectividad

Operacional:

En los sistemas de reconocimiento facial existen ciertas restricciones que son impuestas para el usuario: un ambiente bien iluminado, el usuario debe mirar directo a la cámara fotográfica para que el sistema pueda analizar e identificar a la persona. Por esto se están desarrollando nuevas técnicas de comparación graficas que disminuirán estas restricciones (Konen, 1996).

El sistema no puede analizar a personas con características físicas, tales como barba, estilo de cabello o con ciertas expresiones faciales. Sin embargo los usuarios encuentran este método muy natural, puesto que serán identificados por su rostro y ésta es la manera más tradicional de la identificación. Es altamente aceptable por los usuarios.

Técnico:

Los sistemas de reconocimiento facial tienen problemas con las tomas en ángulos o con las expresiones faciales que sean un poco diferentes de los usados durante el proceso de codificación. Las plantillas deben ser actualizadas puesto que ocurren cambios en el esqueleto facial durante el proceso del envejecimiento humano.

Aplicaciones en la actualidad:

- Actividades bancarias
- Compañías de tarjetas de crédito
- Seguridad en aeropuertos
- Seguridad para Internet
- Agencias del seguro social
- Seguridad en los edificios

 Instalaciones informáticas
 Compañías telefónicas
 Instituciones de cuidado médico
 Autoridades policiales
 Identificación de terroristas
 Licencias de conducir
 Procesos para registro de votantes
 Sistemas de seguridad social
 Seguridad vehicular

Algunos productos comerciales:

- Facial Data Base Systems (Dectel Security Systems, U.K.)
- True Face, True Face Cyber Watch (Miros, U.S.A.)
- Thermace, VIAS (Forensic Security Services, U.K.)
- FR1000 (Technology Recognition Systems)
- Sherlock Face Recognition (Facial Reco Associates)
- Facial Search System (Identicator, U.S.A.)
- KEN (Lawrence Livermore National Laboratory, U.S.A.)
- MufMaster (NeuroMetric Vision Systems)
- ZN-Face (Zentrum fur Neuroinformatik, Germany)
- FACEit (National University of Singapore)
- ARGUS (George Mason University)
- Face Pass (MIT Artificial Intelligence Laboratory)
- FACE-SOM (UMIST)
- Facial Recognition Software (University of Essex)
- Dextel Crime Net (Dextel Security Systems, UK)
- One on One Facial Recognition Systems (Identification Technologies International Inc., U.S.A)

4.1.4 Geometría de la mano - Patrones de las venas

Este método biométrico se basa en distintas características de las manos, que incluyen: contorno externo, líneas internas, geometría de la mano, longitud, patrón del vaso sanguíneo en la parte posterior de la mano, el tamaño de los dedos, de la palma y de las huellas dactilares. Trabaja comparando la imagen de la mano con la muestra previamente guardada. El usuario incorpora su número de identificación en un teclado numérico y coloca su mano sobre una placa. Una cámara fotográfica captura la imagen de la mano y entonces un software la analiza. Otros sistemas utilizan las tarjetas donde se registra la mano del usuario. Esta tecnología es ampliamente usada en control de acceso.

Efectividad:

Técnico:

Los sistemas de la geometría de la mano son razonablemente rápidos, requieren poco espacio para el almacenaje de datos y utilizan poco tiempo para la verificación.

El funcionamiento de estos sistemas se puede ver perturbado si el usuario usa anillos grandes, tiene los dedos hinchados o le faltan los dedos. La suciedad puede también obscurecer la interpretación de los detalles de la mano. La reconstrucción de la estructura de los huesos de la mano de un usuario autorizado puede engañar al sistema. Los sistemas que miden tres dimensiones de la geometría de la mano aunque son más seguros, no son infalibles, ya que con una copia exacta se puede burlar al sistema (Sidlauskas, 1987).

La mayoría de los lectores de la mano están diseñados para ser utilizados dentro de ambientes controlados, puesto que bajas o altas temperaturas pueden afectar al sistema. La dirección de la luz solar sobre el equipo puede afectar la fotografía que se toma de la mano. Se han desarrollado varios sistemas para obtener

los patrones de las venas en la parte posterior de la mano. Estos sistemas se basan en convertir los patrones de las venas y digitalizarlas.

Operacional:

Una evaluación de una empresa norteamericana (Holmes, 1991), concluye que el método de la geometría de la mano fue preferido por los usuarios en comparación con la huella dactilar, firma, reconocimiento de la voz, análisis de la retina. Aunque el análisis de la mano es el más aceptable en la mayoría de los países, se encontró que a los japoneses no les agrada colocar la palma de su mano donde la ha puesto otra persona (Newman, 1995). Copias de la estructura del hueso de la mano de los usuarios autorizados, pueden engañar el sistema. Personas con parálisis o con la enfermedad de Parkinson no pueden utilizar este método biométrico.

Aplicaciones en la actualidad:

- Servicios de la inmigración
- Tiempo y atención
- Seguridad en hospitales
- Depósitos
- Casinos (acceso al money room)
- Laboratorios de universidades.
- Actividades bancarias
- Verificación de empleados
- Supermercados
- Farmacias
- Acceso a salas de computación
- Control en prisiones (visitantes)

El proyecto de INSPASS (The Program Immigration and Naturalization Service Passenger Accelerated Service System) utiliza sistemas de reconocimiento de la geometría de la mano en varios aeropuertos de los Estados Unidos para verificar la identidad de los viajeros. Controles de INSPASS han sido instalados en N.Y. (J.F. Kennedy) y en New Jersey (Newark airport) entre otros y de acuerdo a los resultados, la geometría de la mano es la tecnología más conveniente para verificar

los viajeros locales en el control de pasaportes. Pruebas realizadas en varios aeropuertos de los EE.UU. bajo este proyecto justifican esta afirmación.

Roger Kiel, ministro alemán del interior (1995), indicó que la geometría de la mano es la tecnología biométrica preferida para el tráfico de viajeros en los aeropuertos basado en los informes del proyecto de INSPASS.

Algunos productos comerciales:

- Hand Geometry Readers (Computer Data Systems, U.S.A)
- Hand Geometry Readers, ID3D HandKey, HandPunch (Recognition Systems, U.S.A.)
- Digi-2 (BioMet Partners, U.S.A.)
- BioDentity System (Biometric Security Systems, U.K.)
- FastPass II (Biometrics, Inc, U.S.A.)
- Veincheck Systems (British Technology Group, U.K.)
- PG-2001 (Talos Technology Inc, U.S.A.)

4.2 Técnicas biométricas del comportamiento

En esta sección se analizan las técnicas biométricas que miden las características del comportamiento del individuo.

4.2.1 Verificación de la voz

Hay varias características de sonidos, fonéticas y vocales que permiten que un individuo pueda ser identificado. Las características vocales tales como boca, cavidades nasales, la zona de la boca donde se produce el sonido es diferente para cada individuo. Aunque los seres humanos pueden utilizar estas características naturales para identificar a alguien, es muy difícil para un sistema informático analizar las características de la voz.

La persona habla por un teléfono o un micrófono conectado al sistema, entonces el sistema analiza las características de la voz de esa muestra. Generalmente los métodos basados en *la Transformada de Fourier* (ver anexo 3) se aplican para extraer el grupo de características biométricas asociadas a la voz. Éstos son codificados en datos o plantillas. Una de las aplicaciones de codificación es *wavelets* la cual permite descomponer la señal en aproximaciones y detalles, para muchas señales la información más importante se encuentra en las frecuencias bajas, mientras que en las altas frecuencias se encuentran los detalles o matices de la señal. Por ejemplo, en el caso de la voz humana, si eliminamos los componentes con altas frecuencias, la voz suena diferente pero se sigue entendiendo su mensaje, en cambio, si lo que se elimina son las componentes de bajas frecuencias, el mensaje se vuelve irreconocible.

Finalmente el sistema compara las características de la voz contra la muestra grabada previamente. Los sistemas desarrollados hasta ahora no pueden reconocer los cambios de voz producto de los cambios físicos o emocionales. Este método también tiene el problema de la aceptabilidad. Se utiliza sobre todo en control de acceso de sistemas informáticos y telefónicos, en puertas de acceso y en los sistemas de la seguridad de algunos vehículos. Se espera que con la apertura del mercado de las telecomunicaciones por parte de la Unión Europea realizado en 1998, los ministerios de telecomunicaciones hagan legislaciones sobre los servicios de voz y telefonía que permitirán que el mercado de los sistemas biométricos basados en la voz se expanda.

Efectividad

Teórica:

Algunos sistemas se basan en una nueva tecnología llamada TESPAR (Time Encoded Signal Processing and Recognition) que es un lenguaje digital codificado y simple para el habla. Este sistema genera de una forma simple una “firma” en computadora que identifica a cualquier sonido. Trabaja analizando "fotos" de una

onda acústica contra el tiempo sin calcular las frecuencias (algo diferente que el análisis de Fourier clásico). Sin embargo las pruebas matemáticas siguen siendo polémicas. Los sistemas de la verificación de la voz requieren de un muy alto y complejo nivel de computo.

Técnico:

La verificación de la voz no es tan exacta como la verificación biométrica basada en características físicas, sin embargo es aceptada por el público puesto que la voz es la forma más natural de la identificación. Es una tecnología conveniente para los ambientes donde se requieren las "manos libres". Los desarrolladores de los sistemas combinan la verificación del habla con otras formas de seguridad.

A las computadoras se les hace muy difícil filtrar el ruido de fondo. Por otro lado la duplicación de la voz usando una grabadora es una amenaza importante a estos sistemas. Adicionalmente el daño físico o sustracción de estos sistemas puede ocurrir si los dispositivos son localizados.

Operacional:

Enfermedades, fatiga, y tensión son algunos de los factores que causan problemas en los sistemas de verificación del habla. Por otro lado la voz de los individuos cambia con los años lo que hace más difícil verificarla, así que la actualización de las plantillas debe realizarse con regularidad y esto es costoso puesto que es complicado clasificarlas.

Sin embargo, este sistema es menos vulnerable al acceso desautorizado que las tarjetas, ya que éstas pueden ser perdidas y las contraseñas o los PIN pueden ser robados. La verificación del habla puede hacer de un sistema de seguridad menos vulnerable a la violación y más fácilmente accesible desde sitios remotos. Algunos sistemas tienen procedimientos tediosos al registrar los usuarios.

Las mujeres tienen frecuencias más complejas en la voz que las hace más complicadas para ser identificadas. Personas con problemas de la garganta o incapaces de hablar no pueden utilizar tales sistemas. Personas afectadas por el alcohol, anestesia dental o alguna obstrucción oral pueden encontrar dificultades en ser verificado por estos sistemas.

Aplicaciones en la actualidad:

- Sistemas anti-hurto para los vehículos y las puertas de acceso
- Control de acceso del PC y de ordenadores de la red
- Sistemas de la entrada de la puert
- Hospitales (acceso al cuarto de niños)
- Telefonía
- Equipo para autorizar tarjetas magnéticas
- Control de pasaportes
- Teléfonos en prisión
- Farmacias
- Compañía aeroespacial
- Fuerza aérea en comunicaciones del aire (identificación de pilotos)
- Universidades (acceso a los laboratorios, a los centros de computación, etc.)

Algunos productos comerciales:

- VOCAL, VOCAL SCW1, VOCAL ZKE (ABS, Germany)
- PIN-LOCK, voice verification system (T-NETIX, U.S.A.)
- Caller Verification System (Bell Security, U.K.)
- Tele-MAtic (Speakez, U.S.A.)
- TESPAR/FANN (Domain Dynamic Limite, UK).

4.2.2 Verificación manuscrita de la firma

Este método biométrico se basa en el hecho de que la firma es una acción refleja, no influenciada por control muscular deliberado y con ciertas características

(los ritmos, toques sucesivos de la superficie por la escritura, velocidad y aceleración).

Los sistemas basados en este método biométrico caen dentro de estas dos categorías:

- Los sistemas basados en bolígrafos que utilizan plumas especiales para capturar la información.
- Sistemas basados en tabletas con superficies especiales para recoger los datos.

En el primer sistema la pluma es el aparato de medición que captura la información y en el segundo sistema, la tableta contiene el aparato de medición. Dependiendo del sistema, tanto la superficie donde se firma como el bolígrafo utilizado pueden contener varios sensores. Estos sensores miden características mucho mas allá que simplemente la forma o apariencia de la firma: la presión que se aplica sobre la superficie, el ángulo al cual se sujeta el bolígrafo y hasta la velocidad y el ritmo de cómo la persona ejecuta su firma son características capturadas por el sistema. Algunos de los sistemas antedichos utilizan métodos estadísticos para verificar la firma, otros utilizan métodos de eventos secuénciales. Entre los aspectos tomados en cuenta para realizar un análisis estadístico se incluyen:

- Tiempo total para escribir una firma.
- Mediciones del número de espaciamientos y punto de giros horizontales.
- Número de veces
- Duración en que la pluma toca la tableta.

En métodos de eventos secuenciales, el sistema divide la firma en eventos independientes y examina cada pedazo por separado. Un número de firmas (dependiendo del sistema) se requieren para el proceso de registro. A la hora de la verificación se le pide el usuario firmar. El sistema compara varios aspectos de su firma en una manera jerárquica. Si una buena concordancia no se encuentra entre las características de las firmas (forma, secuencia de evento, características locales)

y la plantilla, entonces se rechaza la plantilla, el uso de redes neurales hace de estos sistemas más exactos y más económicos.

Efectividad

Operacional :

Puesto que la firma es una manera familiar de identificar a individuos, los sistemas de verificación de la firma son altamente aceptables. Una prueba que realizó una compañía británica de correos, mostró que el sistema de verificación de firma fue el preferido sobre el sistema de la huella digital. Sin embargo las personas con la enfermedad de Parkinson no pueden utilizar este sistema.

Algunos sistemas tienen dificultades con las personas que cambian su firma muy radicalmente. Sin embargo existen otros sistemas más sofisticados (como por ejemplo Securisign) que puede prevenir el acceso de personas que estén bajo influencia de drogas o del alcohol. Estos sistemas son costosos ya que requieren hardware de un alto nivel de procesamiento.

Aplicaciones en la actualidad:

- Actividades bancarias
- Servicios de renta pública
- Correos
- Asistencia social
- Compras caseras
- Seguro social

Algunos productos comerciales:

- Signature Analyzer (PenOp Inc., U.S.A.)
- Rolls Royce Signature Verification (British Technology Group, U.K.)
- Electronic Signature Verification System (Quintet, U.S.A.)
- Cyber-SIGN (Gadix, U.S.A.)
- Signature Verification Software (Communication Intelligence Corp., U.S.A.)

- Countermatch (AEA Technology, U.K.)
- ID-007 (cadix International, Japan)
- IBM Transaction Security System (IBM. U.S.A.)
- Sign/On (Checkmate Electronice, U.S.A.)

4.2.3 Verificación del tecleado

Este método que está en el desarrollo se basa en las características mecanográficas de los individuos, tales como presión del teclado, tiempo de tecleado, frecuencia de error en la mecanografía, fuerza en el tecleado, etc.

Dos clases de sistemas están siendo desarrollados basados en técnicas estáticas y dinámicas de verificación. Las aplicaciones mediante verificación estática se aproximan a una red neural, mientras que el verificador dinámico utiliza la estadística. En el método estático el sistema analiza la manera en que el nombre del usuario o password fue mecanografiado, usando la red neural para el reconocimiento de patrón. En el método dinámico el sistema verifica la persona continuamente con cualquier entrada de texto arbitraria.

Éste es un método que se puede ofrecer como suplemento a sistemas de seguridad para la autenticación, pero no se debe utilizar de forma independiente. El funcionamiento del método se ve afectado por varias circunstancias, tales como lesión de la mano o fatiga del usuario legítimo. Los sistemas desarrollados para este método biométrico son costosos, puesto que utilizan métodos neurales y terminales dedicados. Algunos de los productos desarrollados para la dinámica del tecleado son: BioPassword Security Systems, Reino Unido, Electronic Signature Lock Marketing, EE.UU. y M&T Tecnologics, EE.UU.

4.3 Nuevas técnicas biométricas

En esta sección describiremos técnicas biométricas más recientes, de las cuales algunas todavía están bajo desarrollo.

4.3.1 Patrón del ADN

Este método se basa en diversos patrones biológicos de la molécula de ADN en los individuos. Existen diferencias únicas en el patrón de los fragmentos de las bandas de ADN. Las impresiones del ADN fueron utilizadas primero en el Reino Unido en 1983.

La estructura molecular del ADN se puede comparar con una cremallera, en la cual cada diente está representado por una de las letras: A (Adeline), C (citosina), G (guanina), T (Timina) y con los dientes opuestos que forman uno o dos pares de A-T o C-G. La información del ADN es determinada por la secuencia de letras a lo largo de la cremallera. A diferencia de la huella dactilar que ocurre solamente en los dedos, la impresión del ADN es igual para cada célula o tejidos del cuerpo humano.

Este método se utiliza extensamente para identificar criminales. Las desventajas básicas contra este método es la aceptabilidad ética y práctica del usuario. La cantidad de tiempo para verificar a un individuo es también una desventaja grande, puesto que la prueba de ADN no es realizada en tiempo real y es muy intrusiva. El reconocimiento del patrón de ADN, es un procedimiento de laboratorio que sigue los siguientes pasos:

- Aislamiento del ADN.
- Corte, dimensionamiento y clasificación.
- Transferencia del ADN.
- La prueba.

Es un método costoso que requiere el suministro o muestra de tejido humano. Muchas personas lo consideran muy denigrante y generalmente es usado para casos de criminología.

4.3.2 Reconocimiento por medio de los poros sudoríficos

La distribución de los poros en el área del dedo es distinta para cada individuo. Basados en esta observación, analizadores de los poros de sudor de la punta de los dedos han sido desarrollados. Cuando el dedo se coloca en el sensor, el software registra los poros como estrellas y almacena sus posiciones relativas en el área del dedo. Un sistema de este tipo esta siendo desarrollado por la empresa Personal Biometric Encoders, U.K. con el nombre de PCMCIA.

4.3.3 Reconocimiento por medio de la forma y tamaño del oído

La forma y tamaño de los oídos son características únicas de cada individuo. Esta técnica es utiliza por ciertos policías para identificar a criminales. La empresa *ART Techniques* comercializa el producto *Optophone Ear Shape Verifier* que permite realizar este tipo de reconocimiento.

4.3.4 Reconocimiento por detección del olor

La premisa de esta técnica es que químicos llamados "*rolatiles*" producen el distintivo olor de las personas. Un número de sensores está comprobando los diversos compuestos que producen el olor de las personas, este método está en desarrollo y existe un proyecto llamado Scentinel (Mastiff Electronic, U.K., Davis, A 1997) que investiga sobre la posibilidad de identificar al individuo a través del olor.

4.4 Análisis de los métodos biométricos

Cada técnica biométrica tiene diferentes ventajas y desventajas, las cuales tiene diferentes pesos dependiendo de su aplicación. La siguiente tabla explora los parámetros que definen la aplicabilidad de varios métodos biométricos y genera una puntuación total (en base a 10 puntos). El sistema biométrico ideal es definido como

no intrusivo, muy seguro, económico, fácil de usar y con una puntación máxima de 10 puntos (ver tabla 3).

METODO DE AUTENTIFICACION	NO-INTRUSIVO	SEGURIDAD	ECONOMICO	FACIL	PUNTUACION
Sistema biométrico ideal	10.0	10.0	10.0	10.0	10.0
Identificación numerica personal (PIN)	10.0	1.0	9.5	4.5	6.3
Escaneo de la huella digital	4.5	7.0	6.5	5.5	5.9
Reconocimiento de la voz	8.0	4.0	8.5	2.5	5.8
Escaneo del iris	2.5	9.8	1.0	9.5	5.7
Digitalización de la firma	9.5	2.0	7.5	3.5	5.6
Geometria de la cara	6.0	4.0	5.5	7.0	5.6
Geometria de la mano	4.0	4.2	4.5	5.5	4.6
Retina	0.5	9.0	3.5	1.0	3.5

Tabla 3. Comparación de los sistemas biométricos (International Biometric Industry Association, 2001)

Una gran variedad de técnicas biométricas es usada actualmente y para reconocer las fortalezas y debilidades, se presenta a continuación el resultado del estudio realizado por Gartner Dataquest (Junio 2001), ver tabla 4:

SIST. BIOMETRICO	FORTALEZAS	DEBILIDADES
Huella digital	• Una forma natural de tomar medidas biométricas. • Confiabilidad aceptable • Gran cantidad de marcas • Bajo costo • Bajo FAR • Plantillas pequeñas (menos de 500 bytes)	• Alto potencial de FRR, causado por presionar muy fuerte el dedo, alinearlo mal, suciedad y cicatrices • Su asociación con la detención de criminales • Incompatibilidad entre marcas • Requiere contacto físico (negativo en Japón)
Geometría de la mano	• Plantillas pequeñas (10 bytes) • Fácil de usar • Baja tasa de fallo al inscribirse • No se ve afectado por ninguna condición de la piel	• Tamaño físico del equipo • Alto riesgo de FAR • Crecimiento juvenil de los dedos • Requiere contacto físico (negativo en Japón)

Tabla 4. Fortalezas y debilidades de los sistemas biométricos

SIST. BIOMÉTRICO	FORTALEZAS	DEBILIDADES
Reconocimiento facial	• Fácil de usar • No-intrusivo • Amplia aceptación	• No puede distinguir gemelos idénticos
Iris	• Estable en el tiempo • Amplia base de datos • Bajo FAR	• Alto costo del hardware • Requiere entrenamiento del usuario • Intrusivo, resistencia por parte del usuario
Retinal	• Estable en el tiempo • Amplia base de datos • Bajo FAR	• Alto costo, utiliza iluminación especial • Requiere entrenamiento del usuario y su cooperación • Muy Intrusivo, resistencia por parte del usuario • Lectura lenta • Puede revelar otras condiciones medicas
Firma	• Aceptado por el usuario • No se requiere entrenamiento • Bajo costo • No-intrusivo	• La firma varia en el tiempo • No recomendado para usuarios con firma errática • La firma puede variar dependiendo de la emoción o la salud • La inscripción toma tiempo
Voz	• Bajo costo • No-intrusivo • Aceptado por el usuario • Bajo entrenamiento	• La voz varia con el tiempo, por ejemplo, atravesar una enfermedad o estrés • Puede ser burlado por una voz grabada • No es adecuado para reconocimiento • Depende de micrófonos • Plantillas grandes: 64 Kb

FAR = Tasa de falsa aceptación FRR = Tasa de falso rechazo Fuente: Gartner Dataquest (Junio 2001)

El escaneo de la huella dactilar y la geometría de la mano son ampliamente aceptadas por el público, mientras que la tecnología del iris y de la retina no tanto, pero son utilizadas para aplicaciones de alta seguridad. La tabla 5 resume las aplicaciones típicas de algunos sistemas biométricos.

Tecnología Biométrica	Principal Aplicación
Escaneo de la huella dactilar	Accesos a redes, acceso físico, automóviles.
Geometría de la cara	Seguridad en aeropuertos, identificación de criminales
Escaneo del iris o retina	Acceso de alta seguridad para servicios del gobierno o financieros
Geometría de la mano	Acceso físico.
Reconocimiento de la voz	Terminales móviles, telefonía bancaria.
Digitalización de la firma	Actividades bancarias

Tabla 5. Aplicaciones típicas de algunos sistemas biométricos (Dataquest, 2001)

A diferencia de la autenticación por medio del PIN o password, la identificación y autenticación biométrica no requiere una exacta coincidencia. Las tasas de falso rechazo y falsa aceptación cuantifican la exactitud del sistema biométrico. A continuación se muestran en la tabla 6, los valores de exactitud de los principales sistemas.

Biométrico	Tasa de fallas
Escaneo de la retina	1 : 10,000,000+
Escaneo del iris	1 : 131,000
Huella digital	1 : 500
Geometría de la mano	1 : 500
Firma	1: 50
Voz	1 : 50
Reconocimiento facial	1 : 88

Tabla 6. Valores de exactitud de los principales sistemas biométricos. (Biometric Techology, Inc., 2001)

De todas las técnicas biométricas enumeradas en la tabla, sólo la firma y la voz se basan en características del comportamiento en lugar de características físicas. La voz y la firma de las personas están propensas a la variabilidad en la ejecución y, en el caso de la voz, la variabilidad también depende de los instrumentos usados para tomar la medida. Es por estas razones que dichos métodos tienen muy baja exactitud.

4.5 Discusión de los sistemas biométricos

Después del ataque terrorista del 11 de Septiembre 2001 en New York, nuevas directrices basadas en tecnología biométrica comenzaron a ser consideradas por el congreso norteamericano. La biometría aparece en las nuevas leyes antiterroristas, pero las pruebas de los expertos demuestran que engañar a la biometría es, por el momento, bastante sencillo.

La institución sin fines de lucro RAND (siglas que proviene de la contracción *Research and Development*), publicó en el 2001 el informe "Biometrics: Facing up to terrorism", firmado por John Woodward, funcionario de la CIA, quien recomienda la biometría para "controlar el acceso a sitios vitales como aeropuertos, reducir el fraude en documentos de inmigración e identificar a sospechosos terroristas con tecnologías de reconocimiento facial".

Siguiendo esa misma línea, el congreso norteamericano instaba a la introducción del reconocimiento dactilar y de manos en las licencias de conducir y de inmigración, con la creación de una gran base de datos de huellas de ciudadanos.

Otra ley, la "Enhanced Border Security and Visa Reform Act" ordena que a partir de octubre del 2003 se expidan visados biométricos para los 250 millones de extranjeros que entran cada año en EE.UU. Por otro lado el Congreso encargó al National Institute of Standards and Technology (NIST) una evaluación de las posibilidades de la biometría en una de las leyes antiterroristas más importantes: la "USA Patriot Act".

Según el NIST, "el reconocimiento de huellas dactilares funciona bien, pero debe mejorar mucho para usarse a escala masiva; las tecnologías de reconocimiento facial no están aún maduras y el escáner de iris se basa en tecnología propietaria que hace difícil la evaluación de su exactitud. Ningún sistema biométrico funciona

suficientemente bien como para que podamos fiarnos sólo de él. Siempre parecen más fuertes y fáciles de lo que son en la práctica".

Los expertos coinciden con el NIST. Según el director del centro biométrico de la Universidad de San José, Jim Wayman, "el despliegue gubernamental es sólo humo, la probabilidad de que el terrorista Osama Bin Laden pueda ser identificado en un aeropuerto es del 60%". Edward Gareth, de la empresa Image Metrics, añade: "Para detectar al 90% de terroristas, la alarma sonaría erróneamente una vez de cada tres. Es inconcebible construir un sistema de seguridad efectivo en estas condiciones".

El aeropuerto de Palm Beach (Florida) experimentó con un sistema de reconocimiento facial que debía identificar a quince empleados repartidos por las terminales. Consiguió un 47% de éxitos y falló cuando había cambios de luz o alguien se movía. El aeropuerto desistió de sus planes biométricos. A pesar de ello, el Pentágono ha dedicado 42 millones de dólares a un programa para la identificación de personas en las embajadas estadounidenses.

Los primeros avisos contra la falsa seguridad de la biometría vinieron de los científicos. Un matemático japonés Tsutomu Matsumoto (2002), burló a los sistemas de reconocimiento dactilar con un dedo artificial hecho con gelatina para dulces. Le puso unas huellas legítimas, extraídas de un vaso, y engañó a los sistemas más sofisticados en un 80% de ocasiones, incluidos los que aseguraban llevar "reconocimiento termal". Precio del experimento: diez dólares. Este caso se encuentra documentado en la ITU (International Telecommunication Union) en la siguiente dirección http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.html.

Tsutomu Matsumoto duplicó una huella dactilar resaltando su impresión sobre cristal (por ejemplo, un vaso o una ventana) mediante adhesivo de cianoacrilato y fotografiando el resultado mediante una cámara digital. La imagen resultante se

mejoró mediante una aplicación procesadora de imágenes (PhotoShop) y se imprimió en una hoja de papel transparente. Matsumoto utilizó dicho papel como máscara para generar un circuito impreso con la imagen de la huella dactilar (para proporcionar "relieve"). Seguidamente se obtuvo un dedo de "gelatina" empleando el circuito impreso para proporcionarle el relieve que emula la huella digital. En total, menos de 10 dólares en gastos y una hora de trabajo. El resultado: un "dedo" que pasa la prueba de un escáner digital con una efectividad del 80%.

Por otra parte la revista alemana "C't" publicó un test en Octubre del 2002 realizado por Lisa Thalheim, Jan Krissler y Peter-Michael Ziegler donde se evaluaron once dispositivos comerciales. El resultado fue que todos fueron burlados. Los sistemas faciales fallaron al dar por buena la foto o el vídeo de la cara de una persona. Para engañar a los escáners de iris, fue suficiente una fotografía de alta resolución del ojo legítimo, con un agujero en el medio. Los investigadores pusieron detrás su propia pupila, para simular que el ojo fotografiado estaba vivo. En cuanto al reconocimiento dactilar, algunos sistemas fallaron sólo respirando encima de las huellas dejadas en el mouse por el usuario legítimo, o bien aplicando sobre ellas una cinta adhesiva o una bolsita con agua tibia. "Aunque los fabricantes presenten sus aplicaciones como maduras y seguras, el mercado masivo para esta tecnología está aún en su infancia", concluían los periodistas de la revista.

El experto en seguridad Bruce Schneier (1999) ha también llamado la atención contra la biometría: "Por seguridad, nunca debe tenerse una misma contraseña para dos sistemas diferentes. Pero, cuando use mi dedo para poner en marcha el coche, acceder a mis datos médicos, leer el correo... si me roban los datos dactilares no podré cambiar de dedo como de contraseña: …qué pasará entonces". Critica además que en muchos sistemas la información biométrica guardada en el computador o enviada a la red no va cifrada, lo que podría permitir a un atacante apoderarse de los datos.

Diversos grupos de cyberderechos han denunciado los problemas de privacidad de la biometría, tanto por estos robos de información como por la creación de bases de datos con caras o huellas dactilares, contra las que se verifican las identidades. Oliver Tattan, de la empresa Daon, afirmó en Agosto 2002 que, para el éxito de la tecnología, "es urgente la creación de una infraestructura de confianza biométrica mundial, que permita a las empresas y gobiernos identificar a la gente que se mueve de un país a otro".

Para muchos expertos la biometría es aún un juego de niños, un sector muy experimental, ya que el principal problema son los errores de precisión, que pueden llevar a una falsa aceptación o un falso rechazo. Eso está impidiendo su despliegue, aunque sabemos que esto mejorará. El precio es otra barrera: un escáner de lectura dactilar para PC, por ejemplo, cuesta alrededor de 225 dólares, que multiplicados por los cien computadores que puede tener una empresa se obtiene una cifra importante.

Antonio Villalón autor del libro "Seguridad en UNIX" y miembro de la Agrupación de Biometría Informática Española, comenta: "Los sistemas biométricos no deben usarse solos, sino junto a otros modelos de autenticación, como claves o tarjetas inteligentes. En cuanto a la privacidad, ¿qué sucede si, cuando abres una puerta, el escáner de huellas envía tu patrón a una base de datos central? ¿Y si a partir de tu retina se puede determinar que has consumido drogas o padeces una enfermedad? En el momento en que aceptamos pasar por el escáner perdemos el control". A pesar de ello, Villalón está convencido de que "la biometría va a prosperar mucho. “Hubo un boom y cuando se ha visto que no es infalible, se ha pasado a criticarla, pero no existe ningún producto mágico que garantice completamente la seguridad sino que hay muchos, combinados entre sí. Evidentemente, una contraseña se puede cambiar si es comprometida, mientras que unos ojos o una mano, no. Pero, de la misma forma, no te pueden robar los ojos, ni te los olvidas en casa".

Es cierto que utilizando seguridad biométrica de reconocimiento de la huella dactilar nos arriesgamos a que nos puedan amputar un dedo, o a que nos copien nuestra huella dactilar de un vaso para hacer un molde. Sin embargo, ¿hasta qué punto con sólo hacer un molde de la huella es suficiente para engañar el sistema?

En el caso de un entorno altamente seguro, existen sensores que detectan vida en el dedo y son los más adecuados para utilizar en entornos donde se requiere un alto nivel de seguridad.

El tipo de solución de seguridad a implementar dependerá de lo que se pueda obtener al intentar engañar el sistema. No se utilizará la misma solución biométrica para proteger los PC´s de una oficina que para proteger el acceso a la caja fuerte de un banco. En el primer caso, se tendrá en cuenta la comodidad para el usuario como un elemento de peso: no tener que acordarse de complicados passwords y no tener que actualizarlos cada tres meses. Con esto no se pretende decir que la biometría no tenga que ser un sistema seguro sino que no es la única ventaja competitiva que ofrece frente a su sustitutivo (sistema de passwords). Si se analiza, sigue siendo más fácil copiar un password que copiar una huella dactilar en un entorno formado por usuarios con conocimientos medios de informática. A diferencia de los passwords, la biometría sigue añadiendo seguridad, comodidad y ahorra costos derivados de la administración del sistema de passwords de la empresa. Por otro lado, en el control de acceso a la caja fuerte del banco, se deberá optar por una solución biométrica de alta seguridad, como por ejemplo tarjeta que integre un sensor de huella dactilar que detecte vida.

En conclusión, todas las tecnologías biométricas tienen sus puntos fuertes y sus puntos débiles. La tecnología basada en el reconocimiento del iris es una de las más confiables pero también una de las más caras y más intrusivas. Se trata de elegir la que para el entorno en particular, las ventajas superen a los inconvenientes. Por ejemplo, en el caso de un acceso restringido a una sala de pruebas de un laboratorio, una autenticación fuerte sería una buena solución. Otra alternativa podría ser la combinación de varias tecnologías como la del iris y la huella dactilar.

Por otro lado, hoy por hoy existen tecnologías mucho más perfeccionadas y confiables. Una vez elegida la tecnología, en todos los casos se deberá analizar cuidadosamente el producto y asegurarse que se cumplen todos los tests de confiabilidad que ha realizado el fabricante.

La biometría es una tecnología que añade seguridad a los sistemas tradicionales de passwords y tarjetas, complementándose muy bien con otros sistemas de seguridad como el PIN. Sin embargo, se debe tener en cuenta que no todas las tecnologías ni todos los productos del mercado ofrecen las mismas garantías, al igual que pasa con todos los demás productos de otros mercados. Se debe conocer a fondo las necesidades y requisitos del cliente para poder implementar con éxito un proyecto biométrico.

CAPITULO V

EXPERIMENTO

5.1 Experimento realizado para engañar un mouse biométrico

Inspirados en el trabajo del japonés Matsumoto y en el artículo de la revista C't, se decidió intentar engañar un sistema biométrico. Para ello se utilizó un mouse marca BioLink que escanea la huella digital y que es usado para el control de acceso en computadoras. Este mouse trae un software de demostración que fue de gran utilidad, ya que permite registrar usuarios para luego verificar si reconoce o no a los usuarios que intentan ingresar en el sistema. Dicho software muestra en pantalla una imagen de la huella digital escaneada y el nombre del usuario (si este fue reconocido por el sistema) tal como se muestra en la siguiente figura:

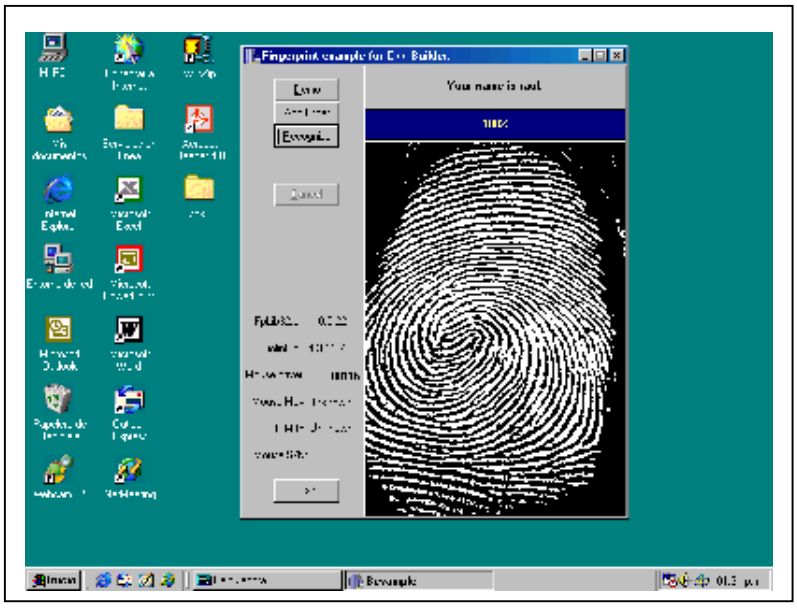


Figura 34. Imagen de la huella digital escaneada por el mouse digital

El protocolo de reconocimiento de la huella digital está escrito en lenguaje *Borland C*. El mouse U-MATCH BioLink de dos botones para computadoras, funciona con un pequeño escáner y el software verifica la huella digital del usuario, actuando como una "llave de seguridad", permitiendo únicamente el acceso al computador o a la red a personas debidamente autorizadas.

Figura 35. mouse U-MATCH BioLink

La comparación directa entre la imagen de la huella a ser identificada y las numerosas imágenes almacenadas, no servirían para una comparación confiable, debido a su baja tolerancia a los errores (Ej. ruidos en la imagen, áreas de la huella dañadas, o diferentes posiciones en la postura del dedo, ángulos de orientación o deformaciones del dedo durante el proceso de toma de imagen). La solución a este problema es extraer características de los llamados “puntos de minucia” (puntos donde las líneas dactilares tienen bifurcaciones o terminaciones) a partir de la imagen de la huella, y comparar entre estos conjuntos de características. El mouse U-MATCH BioLink utiliza la tecnología TSR (Triple Screening Recognition), la cual permite leer tres veces la huella digital del usuario, antes de darle acceso al sistema.

La huella digital del usuario nunca se captura como imagen sino como “puntos de minucia”, ocupando solamente 500 bytes de memoria, de tal manera que no permite duplicar una impresión dactilar. El sistema emplea una serie de soluciones algorítmicas que mejoran el rendimiento y la confiabilidad. Para ello utiliza un algoritmo de filtrado de imagen que permite la eliminación de ruidos, y extrae los puntos de minucia, aun desde imágenes de baja calidad. En la figura 36 se puede observar, la imagen original de la huella y la misma imagen luego del filtrado y procesamiento (con la posición y dirección de la minucia marcada por círculos y líneas).

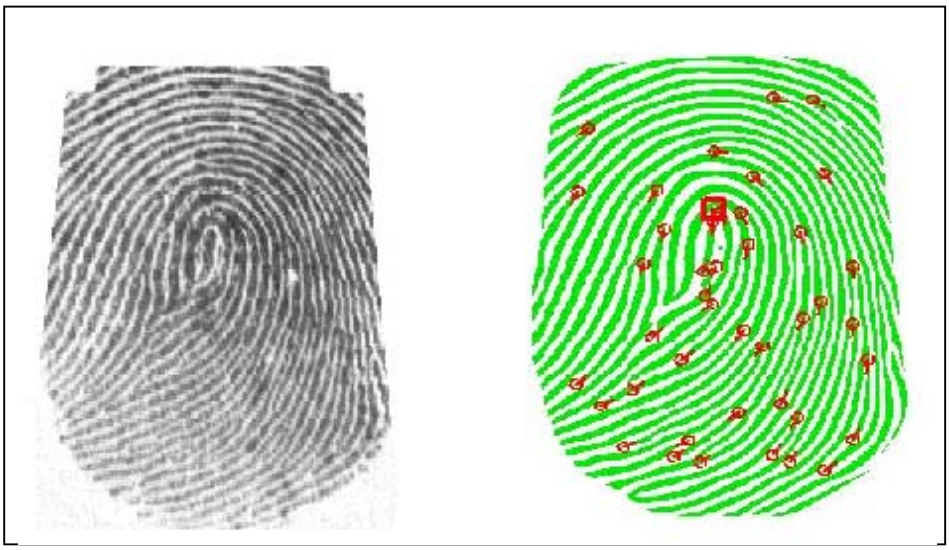


Figura 36. Imagen original de la huella y la misma imagen luego del filtrado

El mouse U-MATCH BioLink puede ser utilizado en verificación 1:1 ó reconocimiento 1:n. Toda la base de datos está preordenada utilizando ciertas características globales. La comparación es realizada primero contra las huellas almacenadas que contienen similares características globales a la que se está evaluando. Si la comparación contra este grupo no arroja resultados positivos, el próximo registro con características globales similares es seleccionado, y así continua hasta que el reconocimiento es positivo o hasta que se llega al final de la base de datos. En la mayoría de los casos hay una alta probabilidad de que el reconocimiento exitoso se alcance al comienzo de la búsqueda lo que reduce la cantidad de comparaciones requeridas para alcanzar un reconocimiento exitoso y consecuentemente, la velocidad de respuesta efectiva es mejor.

El mouse U-MATCH BioLink registra por generalización de características a partir de tres imágenes de la misma huella (TSR). Cada imagen es procesada y sus características son extraídas. Luego las tres colecciones de características son analizadas y combinadas en una sola colección, que es la que se escribe en la base de datos. De esta manera la minucia registrada es más confiable y la calidad del reconocimiento es mejor.

Las especificaciones técnicas del mouse son las siguientes:

MARCA Y MODELO:	**BIOLINK, U-MATCH**
TIEMPO DE ESCANEO	**0.13 SEG.**
ÁREA DE LA IMAGEN	**0,71 x 1.1 pulgadas**
RESOLUCIÓN	**440 Pixels per inc (Avg.)**
PUERTOS DE COMUNICACIÓN	**Serial + PS/2**
AMBIENTE	**Temperatura: 40 – 105 °F** **Humedad: 30 %**
REQUERIMIENTOS DEL SISTEMA	**Bajo ambiente Windows,** **Pentium 200 MHz, 32 MB RAM**

5.1.1 El experimento

Luego de instalar el mouse en la PC, se procedió a registrar a 3 sujetos en el sistema (haciendo click en el botón "Add Finger"). Para ello, cada usuario tuvo que colocar el dedo pulgar sobre el escáner del mouse y una vez que el programa registro la huella y se personalizó con el nombre del usuario, se procedió a verificar sí el sistema reconocía a cada uno de los usuarios, siendo positivo para los tres casos.

La primera prueba que se realizó (de manera empírica) para intentar burlar el mouse fue exhalar sobre la pantalla del lector hasta lograr empañarlo para ver si el mouse "leía" la imagen de una huella latente que se había dejando sobre el lector. Todos los intentos fallaron ya que el lector no "veía" ninguna huella que leer (Thalheim, 2002).

Después se intentó vulnerar el sistema mediante una huella digital escaneada e impresa a alta resolución; esta prueba también falló debido a que el lector óptico trabaja mediante la reflexión de la luz y el papel no produce la misma reflexión que la piel.

En vista que no fue tan fácil burlar el mouse como habíamos creído, decidimos hacer un experimento basado en el que realizó Matsumoto (2002), fabricando copias de las huellas digitales de los sujetos registrados en el sistema.

Hay muchas formas de hacer una huella artificial de una original. Primero que nada se debe obtener una copia de la original de un individuo y con esta impresión se crea un molde y luego se genera una huella artificial positiva. En nuestro experimento se procedió de la siguiente manera: para la elaboración del molde, decidimos probar con plastilina común para niños y presionando el dedo pulgar directamente sobre ella se obtuvo una impresión perfecta de la huella (ver figura 37 y 38), por lo que la plastilina funcionó muy bien. Para la elaboración de la huella artificial probamos con varios materiales (silicona, gelatina comestible y cola blanca), ver figura 39 y 40.

5.1.2 Procedimiento

La meta del experimento fue poder fabricar una huella artificial que fuese reconocida por el mouse como la de un usuario registrado en el sistema (ver figuras 41 y 42). A continuación se describe el procedimiento del experimento.

Tipos de huellas artificiales: se fabricaron las huellas digitales de 3 sujetos, utilizando silicona, gelatina comestible y cola blanca.

Tipos de experimentos: se llevaron a cabo 4 tipos de experimentos tal como se describe:

a. Tipo 1: el sujeto presenta su huella dactilar para ser verificada contra su huella real almacenada en el sistema.
b. Tipo 2: el sujeto presenta su huella artificial para ser verificada contra su huella real almacenada en el sistema.
c. Tipo 3: el sujeto presenta una huella artificial para ser verificada contra la huella artificial previamente almacenada en el sistema.

Reglas del experimento: se realizó el experimento bajo las siguientes reglas:

1. Un cuarto sujeto inscrito con su huella digital original sirvió de testigo para la prueba, el cual permitió determinar en todo momento el buen funcionamiento del sistema.
2. Se fabricarían tantas huellas fuesen necesarias (para ir corrigiendo los errores detectados) hasta que la huella artificial sea reconocida por el sistema.
3. Los sujetos utilizarán las huellas artificiales indistintamente sin conocer a quien pertenece.

Sujetos: los sujetos son 3 personas cuyas edades oscilan entre los 25 y 41 años.

Huellas artificiales: las huellas de cada individuo se fabricaron con diversos materiales (silicona, gelatina comestible y cola blanca) ver figura 39 y 40, como se mencionó anteriormente. Una vez obtenido el molde de plastilina, se procedió a rellenar los mismos con los diversos materiales, teniendo mejores resultados con la silicona, aplicada sobre el molde en una capa muy delgada. Es importante destacar que sí la capa era gruesa el sistema no reconocía la huella artificial como alguna existente en la base de datos, lo que no sucedía con la huella artificial de silicona delgada que si era reconocida.

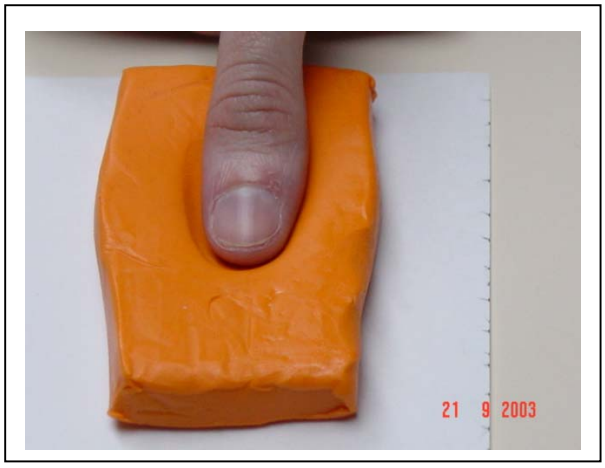


Figura 37. Impresión de la huella digital en plastilina.

Figura 38. Detalle de la impresión dejada en el molde.

Figura 39. Diferentes huellas artificiales elaboradas con distintos productos.

Figura 40. Relleno del molde con silicona.

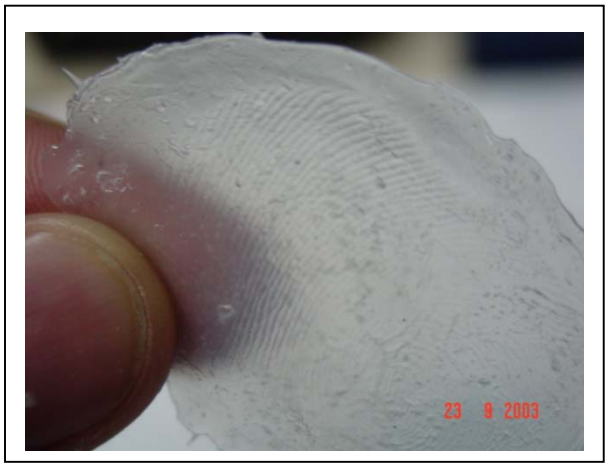


Figura 41. Huella artificial de silicona.

Figura 42. Detalle de huella artificial sobre dedo del sujeto.

Figura 43. Huella artificial sobre el lector del mouse.

5.1.3 Resultados del experimento

Después de fabricar varias huellas artificiales, pudimos determinar que, a pesar que éstas eran copias perfectas de la original, el lector óptico no podía reconocer las huellas artificiales gruesas porque no se amoldaban bien sobre el cristal. El software mostraba un mensaje de error por baja calidad de la imagen capturada. Esto se debió principalmente al grosor con que habían quedado las huella artificiales como se mencionó anteriormente, ya que eran muy rígidas e impedía que se acoplaran perfectamente sobre el cristal del lector, aún ejerciendo suficiente presión.

Para corregir esto, se coloco menos material sobre el molde y se distribuyo sobre él con una capa más fina. Una vez hecho esto, las huellas fueron reconocidas por el mouse sin ningún problema. El sistema reconoció como válidas las huellas artificiales el 100% de las veces para las pruebas tipo 2 y 3.

Figura 44. Huella artificial elaborada con sellador de silicona roja.

Figura 45. Huella artificial realizada con sellador blanco de silicona.

Figura 46. Huella artificial realizada con sellador transparente de silicona

Figura 47. Huella artificial realizada con cola blanca

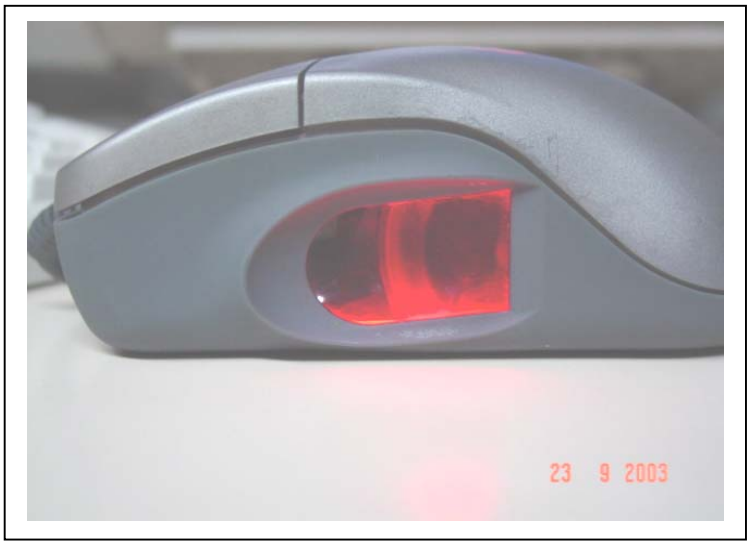


Figura 48. Mouse biométrico activo.

Luego del resultado de las pruebas con el mouse biométrico (ver figura 48) podemos afirmar que éste sistema en particular es vulnerable a que alguna persona ingrese con la identidad del usuario verdadero, por lo que no es recomendable tener solamente este tipo de control de acceso para resguardar información confidencial o de uso restringido.

CONCLUSIONES Y RECOMENDACIONES

- Como todas las tecnologías de seguridad existentes, la biometría es vulnerable.
- La biometría no es un elemento aislado, su eficacia depende del entorno.
- Se debe entender la seguridad biométrica como un elemento complementario en un entorno seguro que añade un nivel más de seguridad al sistema. La biometría por sí sola no es la panacea de la seguridad.
- Para que la biometría cumpla con su función, hay que considerar tres factores fundamentales:
    - *El producto:* el mercado de la biometría es muy amplio y se ha de analizar y probar el producto a fondo antes de integrarlo en el portafolio de soluciones de seguridad. Nunca se debe fiar de lo que dice el fabricante, ya que la mayoría de los tests se realizan bajo condiciones ideales de laboratorio; se debe comprobar las características técnicas del producto. Existen en el mercado más de 400 productos biométricos conocidos y más de 100 empresas que los comercializan.
    - *Los requisitos del cliente*: antes de elegir un producto se han de analizar las necesidades del cliente, el entorno donde se va a utilizar, cuántas personas lo van a utilizar, qué tipo de personas, etc.
    - *No existe una única solución adecuada a todas las necesidades*: no es lo mismo controlar los accesos a las salas restringidas de un edificio que proteger el acceso a los PC´s y redes de la empresa. Dependiendo del caso se puede utilizar contraseña, PIN, autenticación biométrica o la llamada autenticación fuerte, es decir, que una persona se autentique a través de tres elementos: uno que posee (una tarjeta), uno que conoce (un PIN) y uno que es (la característica física).
- Continua siendo más fácil copiar un password que copiar una huella digital en un entorno formado por usuarios con conocimientos medios de informática.

- La biometría es una tecnología que añade seguridad a los sistemas tradicionales de password y tarjetas inteligentes.
- Se debe conocer a fondo la biometría, las necesidades y requisitos del cliente para poder implementar con éxito un proyecto biométrico.
- La técnica biométrica elegida debe proveerle al usuario medidas de privacidad y confidencialidad, y el sistema biométrico no debe registrar la huella del usuario como una imagen sino como un código preferiblemente encriptado, es decir, no debe ser posible reproducir la huella a partir del código matemático creado ni por cualquier otro medio.
- No importa que tan sofisticado sea el sistema biométrico usado ni la complejidad del password, el factor humano suele ser una fuente común de debilidad en sistemas que se piensa que son seguros.
- La aplicación de la biometría no se reduce sólo al control de acceso, sino que es aplicable al comercio electrónico, validación de firmas digitales por medio de una llave biométrica, marketing personalizado, autenticación de personas en aplicaciones de voto electrónico o a través de Internet. La biometría puede ayudar a conseguir mayor seguridad en los sistemas de banca electrónica, comercio electrónico y del sector gubernamental, y el amplio abanico de posibilidades que ofrece esta tecnología podría permite incluso en un futuro, la detección automática de enfermedades, control del estado de animo de las personas, midiendo los marcadores biológicos correspondientes.
- El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptología es también utilizada para el cifrado de la base de datos, o la transmisión entre un dispositivo analizador y una base de datos.
- La autenticación basada en características físicas existe desde que nace el hombre y, sin darnos cuenta, es la que más utiliza cualquiera de nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Obviamente aquí el agente reconocedor lo tiene fácil porque es

una persona, pero en el modelo aplicable a redes o sistemas el agente ha de ser un dispositivo que, basándose en características del sujeto a identificar, le permita o deniegue acceso a un determinado recurso. Si el umbral definido en el sistema es demasiado bajo, se vuelve fácil para una persona no autorizada ser aceptada por el sistema, en cambio si el umbral está demasiado alto, personas autorizadas pueden llegar a ser rechazadas. Los usuarios deben definir estos valores de acuerdo a sus necesidades de autenticar de forma segura la identidad de las personas.

- La falta de estándares no ha permitido explotar al máximo los beneficios de la tecnología biométrica.
- La información que contienen las actuales cédulas de identidad, tarjetas de crédito, etc. se limita a unos cuantos datos digitales, sin embargo los sistemas biométricos ante los que nos haríamos identificar, combinados con un banco de datos harían la información de los usuarios más vulnerables si ocurre alguna falla de seguridad.
- Muchas de las técnicas biométricas ya están siendo utilizadas en sistemas reales, sin embargo, será el futuro inmediato el que nos sorprenderá nuevamente con desafiantes y atractivas aplicaciones basadas en identificación biométrica.

BIBLIOGRAFÍA

Ackerman, Linda (2003), *Biometrics and Airoport Security, Staff Counsel Spoke on Biometrics and Airport Security at the Transportation Research Board (TRB) Panel on Personal Security,* In: Privacy Activism Washington, D.C., January.

Atal, B. S. (1976), **Automatic Recognition of Speaker from their Voices,** Proceedings of IEEE, N° 64, pp. 460-475.

Becerra Yoma, N.; Villar, M. (2000), **Speaker Verification in Noise Using a Stochastic Version of the Weighted Viterbi Algorithm**, Programado para publicación en IEEE Transactions on speech and audio processing, March.

Becerra Yoma, N.; McInnes, F. R.; Jack, M. A. (1998), **Improving Performance of Spectral Subtraction in Speech Recognition using a Model for Additive Noise,** IEEE Transactions on speech and audio processing, Vol. 6, No.6, November, pp. 579-582.

Berouti, M.; Schwartz, R.; Makhoul, J. (1979), **Enhancement of Speech Corrupted by Acoustic Noise,** Proceedings of the IEEE Conference on Acoustics, speech and signal processing, pp.208-211.

Buyer' Guide (1993), *Voice Processing Magazine*, In: Network Buyer's Guide, pp.5-35.

Casacuberta, Francisco; Vidal, Enrique (1987), **Reconocimiento automático del habla,** Marcombo Boixareu Editores, Barcelona España.

CASCADE, (1995), *Chip Architecture for Smart Cards and Secure Portable Intelligent Devices,* In: Esprit Project EP8670, Data Sheet, USA.

Chellappa, R.; Wilson, C. L.; Sirohey, S. (1992), **Human and Machine Recognition of Faces: A Survey**, Proceedings of the IEEE, Vol. 83, pp. 705-741.

Claes, T.; Xie, F.; Van Compernolle, D. (2000), **Spectral Estimation and Normalization for Robust Speech Recognition**, Proceedings of the IEEE International conference on signal processing.

Daugman, J. G. (1993), *High confidence Visual Recognition of Persons by a Test of Statistical Independence,* In: PAMI, Vol. 15, N°. 11, pp.1148-1161, November

Davis, A. (1997), *The Body as Password*. In Wired, March 27.

Davis, H. K.; Biddulph, R.; Balashek, S. (1952), *Automatic Recognition of Spoken Digits*, In: American Journal of Otolaryngology, N° 24, pp. 637-642.

Deller, J. R.; Proakis, J. G.; Hansen, J.H.L. (1993), **Discrete Time Processing of Speech Signal,** New York, MacMillan.

Doddington, G.R. (1985), **Speaker Recognition – Identifying people by their Voices**, Proceedings of IEEE, N°73.

Dudley, H.; Balashek, S. (1958), *Automatic Recognition of Phonetic Patterns in Speech*., In: Journal of the Acoustic Society of America, N°30, pp. 721-739.

Duró Espinosa, V. (2000), **Evaluación de Sistemas de Reconocimiento Biométrico**, Departamento de Electronica, Escuela Universitaria Politécnica de Mataró, Barcelona, España.

Forsyth, M. (1995), **Semi-continuous Hidden Markov Models for Automatic Speaker Verification**, Thesis, The University of Edinburgh, United Kingdom.

Furui, S. (1981), **Cepstral Analysis Technique for Automatic Speaker Verification,** IEEE Transactions on acoustic, speech and signal processing, N°29, pp. 254-277.

Furui, S. (1994), *An O*verview *of Speaker Recognition Technology*, In: ESCA Workshop on Automatic Speaker Recognition, Identification and Verification, pp. 1-9.

Furui, S. (1997), *Recent Advances in Speaker Recognition*, In: Pattern Recognition Letters, N°18 pp. 859-872.

Gareth, Edward (2002), *Security Management: If facial Recognition Bad Medicine*? In: My Report, January.

Gartner Inc. (2001), *Pointing The Finger at Biometric Technology,* In: International Biometric Group, June.

General Accounting Office (1995), **Electronic Benefits Transfer, Use of Biometrics to Deter Fraud in the Nationwide EBT program**, USA.

Gómez, Hernán y Ormella, Carlos (1999), *Autenticación Biometrica*, En: LAN & WAN®, Noviembre, N° 81.

Guerrino, Eric; Kahn, Mike; Kapito, Ellen (1997), **User Authentication and Encryption Overview**, USA.

Hays, R. (1996), **Pasaports into Credit Cards: On the Borders and Spaces of Neoliberal Citienship (INSPASS)**, Universiy of Washington, January, USA.

Hermansky, H.; Morgan, N.; Bayya, A.; Kohn, P. (1991), **Compensation for the Effect of the Communication Channel in Auditory-like Analysis of Speech (RASTA-PLP)**, Proceedings of the Eurospeech, pp 1367-1370.

Higgins, A.; Bahler.,L.; Porter, J. (1991), In: Digital Signal Processing**. Speaker Verification Using Randomized Phrase Prompting**, N° 1, pp. 89-106.

Holmes, J. Wright, L., Maxwell, R. (1991), **A Performance Evaluation of Biometric Identification Devices**, Sandia National Laboratories, U.S.A,

Huopio, Simo. (1998), *Authorization and Access Control in Open Network Environment,* In: Seminar on Network Security, USA.

Irizar, Andoni (1999), *Series y Transformadas de Fourier*, In: Tratamiento Digital de Señal, España.

Jain, A.; Bolle, R.; Pankanti, S. (1999), *Personal Identification in Networked Society,* In: Biometrics, Kluwer Academic Publishers.

Jaypeetex Engieering (2001), *¿Why Ultra Sound?,* In: Products Biometrics.

Jones, D. M.; Hapeshi, K.; Frankish, C. (1990*)*, *Design Guidelines for Speech Recognition Interfaces.* In: Applied Ergonomics, N°20, pp. 40-52.

Konen, W. (1996), **Neural Information Processing in Real World Face Recognition applications**, IEEE Expert, Vol.11, N°4, pp.7-8, August.

Lamel, L. (1981), **An Improved End-Point Detector for Isolated Word Recognition***,* IEEE Transactions on acoustic, speech and signal processing. N° 29 pp. 777-785.

Lea, W. A. (1980), **Trends in Speech Recognition**, Prentice Hall, Englewood Cliffs, N.J.

Lozano, J. F. (2002), **Características Biométricas**, En: Auditoría y Seguridad Informática, pp. 1- 18, España.

McMordie, Dave. (1997), **Texture Analysis of the Human Iris for High Security Authentication**, Technical Report Image Processing pp. 304-529, Department of Electrical Engineering, McGill University, December.

Marin, C.; González, E. (2002), *Prototipo de un Sistema de Seguridad en Ambientes Windows basado en el Reconocimiento de Patrones Biométricos específicamente Reconocimiento de Huellas Dactilares*, En: Tesis, Universidad Central de Venezuela, Facultad de Ciencias.

Marsh, P. (1996), *Biometric Behavior is Smart and Secure*, In: New Electronics, July, pp.25-26.

Mateos Tapiador, M. (1999), **Biometría del Tecleo e Internet**, Programa de Doctorado, Ingeniería Informatica. UAM. Enero.

Matsui, T.; Furui, S. (1993), **Concatenated Phoneme Models for Text-Variable Speaker Recognition***,* Proceedings of the IEEE International conference on acoustic, speech and signal processing, Minneapolis, N° 2, pp. 391-394.

Matsumoto, T. (2002), **Importance of Open Discussion on Adversarial Analyses for Moblie Security Technologies, a Case Study or User Identification***,* Yokohama National University, pp. 1-33, May.

Meenen, P.; Adhami, R. (2001), **Fingerprinting for Security**, IEEE Potentials, pp 33-38, August.

Miller, B. (1994), **Vital Signs of Identity**, IEEE Spectrum, Vol. 31, N°2, pp.22-30.

Montiel, Juventino (1994), **Manual de Criminalística 2,** Editorial Limusa, México, D.F.

Morales, Domingo; Ruiz del Solar, Javier (2000), *Matching de Huellas Dactilares mediante Transformada de Hough Generalizada,* En: Sistemas Biométricos.

Newman, E. (1995), **The Biometric Report**, SJB Services, UK.

NIST, (2002), **Report to the State and Justice Departments for Transmittal to the U.S. Congress**, November.

Olguín, Patrcio (1999), *Sensores Biométricos,* En: Revista Electronica de la Escuela de Ingieneria Electrica, U.C.V., N° 6.

Olóriz Federico (1890), **Técnica Anatómica**, España.

Openshaw, J.P.; Sun, S.P.; Mason, J.S. (1993), **A Comparison of Composite Features under Degraded Speech in Speaker Recognition**, Proceedings of the IEEE international conference on acoustics, speech and signal processing, N°2, pp. 371-374.

Peacocke, R. D.; Graf, D. H. (1990), **An Introduction to Speech and Speaker Recognition**, IEEE Computer, N°23, pp. 26 -33.

Polemi, Despina (1997), **Biometric Techniques: Review and Evaluation of Biometric Techniques for Identification and Authentication, Including an Appraisal of the Areas where They are Most Applicable**, Institute of Communication and Computer Systems National Technical University of Athens, April.

Ruggles, T. (1998). *Comparison of Biometric Techniques*. In: Biometric Technical Assessment, March 27.

Samal, A.; Iyengar, P. A. (1992), **Automatic Recognition and Analysis of Human Faces and Facial Expressions: A Survey**, Pattern Recognition, Vol. 25, pp. 65-77.

Sambur, M. R. (1975), **Selection of Acoustic Features for Speaker Identification**, IEEE Transactions on acoustics, speech and signal processing, N°23 pp. 176-182.

Savoji, M. H. (1989), **A Robust Algorithm for Accurate End Pointing of Speech Signals**, Speech Communication, N° 8, pp. 45-60.

Schneier, Bruce (1999), *Uses and Abuses, Inside Risks 110 CACM*, In: Biometrics N°42, August.

Sidlauskas, D. (1987), **A New Concept in Biometric Identification 3-Dimensional Hand Geometry**, Nucl. Mater. Manage, Vol.16, pp.442-447.

Srinivasan V.S.; Murthy N.N, (1992), **Detection of Singular Points in Fingerprint Images.** Pattern Recognition, Vol. 25, Nº 2, pp. 139-153.

Soong, F. K.; Rosenberg, A. E. (1988), **On the Use of Instantaneous and Transitional Spectral Information in Speaker Recognition**, IEEE Transactions on acoustic speech and signal processing, N°36, pp. 871-879.

Tattan, Oliver (2002), *Biometric Autentication Engine,* In: Biometrics, N°8, August.

Thalheim, Lisa; Krissler, Jan; Ziegler, Peter. (2002), *Body Check: Biometric Access Protection Devices and Programs Put to the Test,* In: Biometrie, c't page 114 – 128.

Toptrend Technologies Corp. (2001), *Fingerprint recognition based on silicon chips* In: Technical Support.

U.S. Congress (2001), *USA Patriot Act of 2001*, In: law H.R. 3162 Section 403.

U.S. Congress (2001), *Secure Transportation for America Act and HR 3165*, *Aviation Security Act II*, In: HR 315031, Octuber.

U.S. Congress (2002), *Enhanced Border Security and Visa Entry Reform Act of,* In: law H.R. 3525.

Vasegui, S. V.; Milner, B. P. (1997), **Noise Compensation Methods for Hidden Markov Model Speech Recognition in Adverse Environments**, IEEE Transactions on speech and audio Processing, N°5, pp. 11-21.

Villalón, Antonio (2002), *Autenticación de Usuarios*, En: Seguridad en UNIX y Redes, Ver. 2.1, Julio.

Wayman, Jim. (2002). *USENIX Security Symposium,* In: Conference at 11th annual.

White G.B.; Fisch E.A; Pooch U.O. (1996), **Computer System and Network Security**, CRC Press.

Woodward, John (2002), *Biometrics: Facing up to Terrorism*, In: RAND corporate, February.

ANEXO 1

ASPECTOS GENERALES SOBRE LA HUELLA DACTILAR

La dactiloscopia es la ciencia que se encarga del estudio de las huellas dactilares y etimológicamente procede del griego *daktilos* (dedos) y *skopien* (observar). Mediante esta ciencia se puede determinar la identidad de un individuo con una certeza casi absoluta (Montiel, 1994).

La estampación de una huella dactilar impregnada en tinta y posada en papel se denomina dactilograma. En las huellas dactilares se pueden distinguir 3 tipos de características:

- **Generales:** Se encuentran en la mayoría de los dactilogramas.
- **Especificas:** Son las empleadas por los expertos para la identificación
- **Individuales:** Determinan la particularidad de cada uno de nosotros. Aportan los puntos característicos, pudiendo aparecer más de cien de estos puntos en una sola huella.

Las huellas dactilares tienen las siguientes propiedades:

- **Inmutables:** no cambian apreciablemente a lo largo de nuestra vida.
- **Perennes:** permanecen en nosotros desde antes de nacer hasta después de nuestra muerte.
- **Diversiformes:** todas las huellas son diferentes entre si. Nunca se repiten.

En el análisis de huellas dactilares podemos diferenciar distintos aspectos: sistemas, fórmula, subfórmula, delta, núcleo y anomalías, los cuales se describen a continuación:

- **Sistemas de crestas papilares**

  - ✓ **Sistema basilar:** Constituido por las crestas de la base del dedo, las cuales van elevándose hasta el tramo superior, donde se encuentran obstaculizadas por una cresta que recibe el nombre de limitante basilar.

  - ✓ **Sistema marginal.** Lo integran las crestas de la parte alta del dactilograma. Comienzan por un lado del dedo paralelamente a las crestas basilares, se apartan de éstas, suben hacia el extremo libre de la pulpa y describen curvas acentuadas con concavidad de cara a la raíz del dedo, y descienden por el lado opuesto al de su inicio. La cresta inferior de este sistema se denomina limitante marginal.

  - ✓ **Sistema nuclear.** Ocupa la parte central y más saliente de la pulpa, circunscrita por los trazos limitantes de los otros sistemas. La cresta interna más próxima a las de los otros sistemas se denomina limitante nuclear.

- **Fórmula**

La fórmula es la serie ordenada de letras y números con los que se representan los tipos de los dactilogramas correspondientes a cada uno de los 10 dedos del individuo.

Se comienza a redactar la fórmula por el dactilograma correspondiente al dedo pulgar de la mano derecha y se continúa en el orden natural que tienen los dígitos en la mano, hasta llegar al auricular; después se repite la operación de idéntica forma desde el pulgar hasta el auricular de la mano izquierda.

Para la codificación de la fórmula es preciso diferenciar el caso de los pulgares del resto de los dedos, utilizándose en cada caso la siguiente codificación:

TIPO	PULGARES	DEMAS DEDOS
Adeltos	A	1
Dextrodeltos	D	2
Sinistrodeltos	S	3
Bideltos	V	4

- **Subfórmula**

Es la subclasificación efectuada en los dactilogramas con el fin de fraccionar los nutridos grupos de tarjetas que producen las fórmulas de mayor repetición.

Cada tipo dactilar tiene una subfórmula adecuada, de tal forma que diremos que la subfórmula en los adeltos es morfológica, la de los monodeltos matemática, y la de los bideltos topográfica

La manera de mostrar gráficamente la subfórmula de cada tipo es mediante números pequeños, letras minúsculas y marcas, que se colocan como denominadores de los quebrados cuyos numeradores constituyen la fórmula.

Los adeltos puros carecen de subformula. Los pseudodélticos se consignan escribiendo una "p" minuscula seguida de la línea infradeltica.

Los monodeltos se subformulan contando el número de crestas existentes entre el delta y la parte central del núcleo (linea de Galton).

En los bideltos se examina cuidadosamente el delta izquierdo hasta determinar cual es la cresta limitante basilar que ayuda a formar el delta. Se propaga esta hacia el delta derecho de forma que al llegar a la altura de éste, si queda más arriba se denomina que es intradelto, si queda a la misma altura mesodelto, y si está por debajo será extradelto. Dependiendo de cuantas crestas haya entre la propagación del delta izquierdo y el delta derecho se dice que es poco, normal o muy intradelto o extrodelto.

Codificación de la subformula de los bideltos:

SUBFORMULA	POCO	NORMAL	MUCHO
Intradelto	(i)	i	i/
Mesodelto		m	
Extradelto	(e)	e	e/

- **Delta**

La convergencia de los tres sistemas de crestas papilares da lugar a la formación de unas figuras llamadas Deltas. Según el número y lugares del dactilograma en los que aparezcan estas figuras, se clasifica el dactilograma de un tipo u otro.

Según el número de deltas, los dactilogramas pueden ser:

- ✓ **Adeltos**. Carecen de estas figuras

- ✓ **Monodeltos**. Aparece una sola figura déltica. Según aparezca a la derecha o izquierda del nucleo se denomina dextrodeltos o sinistrodeltos respectivamente.

- ✓ **Bideltos**. Observamos dos deltas o más. Normalmente serán dos, uno a cada lado del núcleo.

Según el lugar en que aparezcan los deltas, los dactilogramas se clasifican en:

- ✓ **Hundidos**. Se presentan en forma de triangulo pudiendo adoptar distinta morfología (abierto total, abierto superior, abierto exterior, abierto interior, cerrado total, cerrado superior, cerrado exterior, cerrado interior).

- ✓ **Trípodes**. También conocidos como deltas en rama. Se presentan en distintas morfologías (largo total, largo superior, largo exterior, largo interior, corto total, corto superior, corto exterior, corto interior).

- **El núcleo**

Los núcleos de los dactilogramas se clasifican en:

- ✓ **Ansiformes.** Formados por una serie de asas, encajadas unas sobre otras. El asa central se puede presentar en diversas formas: horquilla, horquillas entrelazadas, horquillas gemelas, presilla, interrogación, recto en cresta, centro recto en ojal, centro en fragmento, birrecto, trirrecto, tetrarrecto, pentarrecto, bifurcado, o convergente.

- ✓ **Verticilares**. El nucleo presenta las crestas centrales de forma circular que aparentemente se enrollan dando lugar a una forma

redondeada: circular, elíptica, espiral dextrogira o levogira, gancho dextrogiro o levogiro. Normalmente presentan dos deltas.

- ✓ **Biansiformes.** Aparecen dos asas que se pueden presentar como asas volteadas, nucleos ansiformes de dirección opuesta o de igual dirección.

- ✓ **Mixtos.** Combinación entre ansiformes y verticilares.

Además, un dactilograma puede carecer de núcleo, denominándose anucleado, o poseer una forma rudimentaria de núcleo, sin llegar a ser tal, en cuyo caso se califica al dactilograma como pseudonucleado.

- **Anomalías**

Las anomalías que se presentan pueden ser de dos tipos:

- ✓ **Accidentales:** como pueden ser las siguientes:
  - Desgastes profesionales
  - Callos
  - Hipertrofia
  - Flictemas.

- ✓ **Congénitas**: entre las que destacan:
  - Polidactilia: más de cinco dedos
  - Ectrodactilia: menos de cinco dedos
  - Sindactilia: unión o fusión de dedos
  - Braquidactilia: uno o varios dedos más cortos de lo normal
  - Macrodactilia: uno o varios dedos más grandes de lo normal.
  - Isodactilia: todos los dedos a la misma altura

- Anisodactilia: disposición anormal de los dedos
- Sinfalangia: falta de alguna falange
- Polifalangismo: más falanges de lo normal
- Queratodermia: no hay diferencia entre las crestas y los surcos
- Displasia: desalineamiento de las crestas papilares.

Identificación a través de la dactiloscopia

Fue a mediados del siglo XIX cuando William Herschel demostró la nula alteración sufrida en los dibujos de su dedo índice comparando dos impresiones del mismo con veintiocho años de diferencia e igualmente se percató de las diferencias existentes en los dibujos de los dedos de diversos individuos. A partir de ese momento, con las inestimables aportaciones o investigaciones paralelas de otros personajes, fue cuando se sentaron las bases de la identificación personal a través de las impresiones dactilares, nacía la dactiloscopia. Dada la infinita variedad de modelos existentes, surgieron estudios para la clasificación de los mismos basándose en distintos parámetros.

Los más notables creadores de sistemas de identificación personal fueron: Francis Galton, (Londres, 1885) quien planteaba los fundamentos para la solución del problema que representaba hacer una clasificación de las impresiones dactilares mediante la publicación de su manual *Fingerprint Directories*, el inglés Henry Faulds, (Japón, 1888) realizó valiosos descubrimientos y contribuciones en el campo de la dactiloscopia; uno de ellos fue precisar los tipos de patrón: arco, lazo y espiral presentes en las huellas dactilares, luego, Vucetich (Argentina, 1891) presentó varios trabajos experimentales que se tradujeron en el libro *Instrucciones Generales para el Sistema Antropométrico e Impresiones Digitales*. Tres años después público *Idea de la Identificación Antropométrica*. Cuando ya había conseguido reunir un importante cúmulo de material y había logrado que se conocieran los fundamentos del nuevo sistema identificador, sometió su descubrimiento a la

crítica de los hombres de ciencia de toda Latinoamérica, en el Segundo Congreso Científico Latinoamericano, celebrado en Montevideo, en marzo de 1901. En las resoluciones de ese congreso se determinó invitar a todas las naciones del Continente Americano a adoptar las impresiones digitales como medio individualizador insuperable.

Vucetich concurrió luego al Segundo Congreso Médico de Buenos Aires, presentando allí su trabajo *Dactiloscopía Comparada*, que contenía los fundamentos de esta disciplina y sus relaciones con las ciencias biológicas y establecía comparaciones con los diversos sistemas individualizadores ideados por sus antecesores. Esta obra, de 1904, se considera la principal de Vucetich: recibió premios y menciones en todo el mundo y fue traducida a los principales idiomas, incluso el japonés.

Al celebrarse el Tercer Congreso Científico Latinoamericano, en agosto de 1905, Vucetich presentó su trabajo *Evolución de la Dactiloscopía* destacando que no existían dos personas con iguales huellas dactilares. Sin embargo fue el inglés Francis Galton, fundador de la psicología diferencial basada en el estudio de las diferencias individuales, el descubridor de la exclusividad dactilográfica, escribió el libro *Finger Prints* (1892) donde planteó la necesidad de comprobar tres hechos antes de defender la utilidad de las huellas dactilares en investigaciones criminales o de otro tipo: probar, y no solamente presumir, que una huella se mantiene constante durante toda la vida; que la variedad de huellas es realmente muy grande, y que pueden ser clasificadas o normalizadas de tal manera que cuando un experto examina un conjunto de huellas digitales pueda afirmar, consultando un diccionario apropiado o instrumentos equivalentes, si han sido ya registradas.

Por último se menciona a Federico Olóriz, uno de los grandes genios de la investigación española dejando un legado científico extraordinario en una corta vida llena de trabajo y a quien se le debe el reconocimiento de las

huellas dactilares como método de identificación personal. Sus aportaciones al descubrimiento de la dactiloscopia como método de identificación personal significó un gran paso dentro de la antropología y, especialmente, de la investigación policial, y puede considerarse el creador de la Antropología Social.

A continuación se explica cómo se clasifican los dactilogramas según Federico Olóriz (1890), su método, sin variación alguna, se emplea, además de en España, en Bolivia, Colombia, Perú y Venezuela.

Para una primera clasificación de las huellas dactilares se debe identificar el núcleo y el delta o deltas que aparezcan. El núcleo o sistema nuclear se localiza en la región central de los dactilogramas y es el que ofrece más variedad de dibujos en conjunto y en detalle, debido a la estructura general de su contorno, a la dirección de las crestas que lo integran y a la morfología que muchas de éstas representan. El delta es la fusión o aproximación de los sistemas de crestas papilares (nuclear, basilar y marginal) que dan lugar a un dibujo en forma de trípode o triángulo. Véase figura 49.

Figura 49. Los tres sistemas dactilares y el delta.

El dactilograma de la figura 49 es un claro ejemplo de impresión digital sinistrodelta, el cual se encuentra especificado en la tabla 1, con un núcleo claro y un delta bien definido situado a la izquierda.

La clasificación primaria se realiza basándose en tres factores:

- La presencia o ausencia del delta.
- El número de deltas.
- La posición del delta respecto al núcleo.

La siguiente tabla se emplea para la clasificación y notación de un dactilograma:

Tipo	Delta	Núcleo	Deltas	Posición déltica respecto al núcleo	Fórmula		Color
					Pulgar	Resto	
Adelto	No	No	0		A	1	Carmín
Dextrodelto	Sí	Sí	1	Derecha	D	2	Blanco
Sinistrodelto	Sí	Sí	1	Izquierda	S	3	Negro
Bidelto	Sí	Sí	2	Ambos lados	V	4	Verde

Tabla 7. Clasificación de un dactilograma

Se puede suponer fácilmente que una clasificación en sólo cuatro grupos es del todo insuficiente para la posterior identificación del individuo y por ello existe para cada grupo una ramificación dependiendo de ciertas características:

1. **Adelto.** Pese a que se fija distintos tipos de huellas adeltas, no se van a considerar, dado el escaso número de estos dactilogramas y, fundamentalmente, porque muchos dactiloscopistas tampoco lo hacen.

2. **Monodelto**. La subclasificación es de carácter contable. Localizados el centro del delta y el núcleo se debe trazar una línea imaginaria que los una, esta línea se conoce como *Línea Galtoniana.* Posteriormente se contarán el número de crestas por las que pasa esta línea, sin tener en cuenta aquella que delimita al delta. Véase figura 50.
3. **Bidelto.** La subclasificación es de carácter topográfico. Se debe localizar la cresta que forma la base del delta situado a la izquierda del núcleo. Esta cresta se debe seguir en sentido derecho para determinar qué posición ocupa respecto al otro delta. En el más que probable caso del corte o terminación de esta cresta se seguirá el recorrido por la inmediatamente inferior. Si la cresta de recorrido coincide es la misma que aquella que forma la base del delta derecho, entonces es de tipo mesodelto **[m]**; si queda por encima es intradelto **[i]** (muy intradelto **[i/]** si está a gran distancia del delta y poco intradelto **[(i)]** si está muy próximo al delta); y si se localiza por debajo es de tipo extradelto **[e]** (muy extradelto **[e/]** si está a gran distancia del delta y poco extradelto **[(e)]** si está muy próximo al delta). Véase la figura 51.

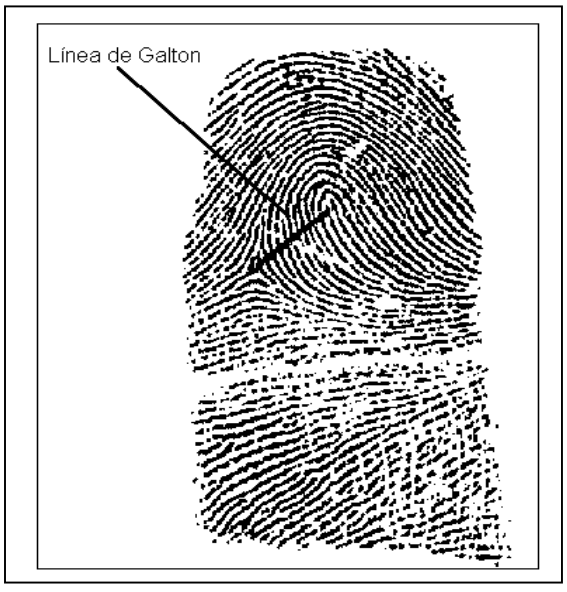


Figura 50. La línea atraviesa once cretas [S|11].

Además, en la subfórmula pueden aparecer los siguientes símbolos:

- **?**, cuando hayan surgido dudas por deficiencias en la calidad del dactilograma.
- **+**, en los monodeltas se añade al lado del número cuando en el dactilograma el núcleo o el delta no aparezcan claros.
- **x**, por aparición de callosidades, cicatrices, ausencia de deltas y núcleos no se haya podido determinar la subfórmula.

Figura 51. Bidelta poco intradelta [V|(i)].

A continuación se presenta la tabla 8 donde se resumen los códigos empleados para la notación de la fórmula y subfórmula dactiloscópicas.

Tipo	Fórmula		Subfórmula	Subtipos	Signo		
	Pulgar	Resto					
Adelto	A	1					
Dextrodelto	D	2	Galtoniana	Número de crestas delto – centrales (1 – 40)	Número		
					+	x	?
Sinistrodelto	S	3	Galtoniana	Número de crestas delto – centrales (1 – 40)	Número		
					+	x	?
Bidelto	V	4	Topográfica	Extradelto	(e)	e	e/
				Intradelto	(i)	i	i/
				Mesodelto	M		
					x		?

Tabla 8. Códigos empleados para la notación de la fórmula y subfórmula dactiloscópicas.

Ejemplo de dos fórmulas dactiloscópicas completas:

$$\frac{S}{16}\,\frac{2}{5}\,\frac{3}{9}\,\frac{3}{14}\,\frac{3}{21} \;\_\; \frac{D}{3}\,\frac{4}{i}\,\frac{2}{7}\,\frac{4}{e}\,\frac{2}{8}$$

$$\frac{V}{(e)}\,\frac{4}{e}\,\frac{4}{e}\,\frac{4}{e}\,\frac{4}{e} \;\_\; \frac{V}{m}\,\frac{4}{i}\,\frac{4}{i}\,\frac{4}{i}\,\frac{4}{i}$$

El método clasificador dactiloscópico se basa en la manipulación de imágenes direccionales creadas a partir de un dactilograma escaneado.

Clasificación

Una vez identificados el núcleo y los deltas marcados, la primera tarea es eliminar los pseudo deltas, es decir bloques marcados como deltas pero que realmente no lo son. Para ello se siguen los siguientes criterios:

1. Si existe más de un delta en la mitad izquierda de la imagen, se conserva el de mayor probabilidad y se elimina el de menor valor.
2. Igualmente para el área derecha de la imagen.

Finalmente, el dactilograma se clasifica siguiendo las siguientes directrices:

1. Si no hay núcleo o éste se ha localizado en una zona impropia, el dactilograma es adelto.
2. Si existe un núcleo bien ubicado y hay un solo delta a la izquierda de éste, el dactilograma es sinistrodelto.
3. Si existe un núcleo bien ubicado y hay un solo delta a la derecha de éste, el dactilograma es dextrodelto.
4. Si existe un solo delta y no ha superado los pasos 2 ó 3, entonces se clasifica a la huella como adelta.
5. Si existen dos deltas, ambos a la izquierda del núcleo, entonces uno de ellos no lo es. Se elimina y se clasifica al dactilograma como sinistrodelto.
6. Si existen dos deltas, ambos a la derecha del núcleo, entonces uno de ellos no lo es. Se elimina y se clasifica al dactilograma como dextrodelto.
7. Si existen dos deltas, uno a la izquierda y el otro a la derecha del núcleo, separados por una determinada distancia, entonces el dactilograma es bidelto.

8. Si existen dos deltas, uno a la izquierda y el otro a la derecha del núcleo, pero están muy próximos entonces el dactilograma es adelto.
9. Si llegados a este punto, no se ha conseguido clasificar el dactilograma, entonces se marca como desconocido (con una equis).

Subclasificación

- **Monodeltos (sinistrodeltos y dextrodeltos):**

  Localizados los bloques que albergan el núcleo y el delta de un dactilograma monodelto, lo primero que hay que realizar es hallar el píxel central de dichos bloques. Seguidamente se traza una línea negra entre ambos, la denominada línea de Galton. Esta línea se va recorriendo y se almacenan en un vector los valores de gris que hay debajo de la misma (guardados en la matriz de la imagen). Tras este proceso resulta un vector con un número determinado de valores de gris. Aquellos valores de gris claros, se hacen blancos. Finalmente, cuando se transite (durante el recorrido del vector) de una zona clara o blanca a una zona oscura se incrementa el número de crestas en una unidad. Debe repetirse el proceso hasta terminar en la última posición del vector. Al número de crestas resultante debe restársele dos, dado que seguramente se contabilizaran la cresta que delimita el delta y la cresta que encierra el centro del núcleo. El valor final corresponde a la subfórmula del dactilograma.

- **Bideltos**

  El método es extremadamente sencillo y no excesivamente efectivo. Sin embargo, en un gran número de casos da buenos resultados. Simplemente se analiza la posición de ambos deltas: si el delta izquierda está por encima del derecho, el dactilograma es intradelto, en

el caso contrario será extradelto. Si están a un mismo nivel, existe la posibilidad de que sea mesodelto. Evidentemente, este método de subanálisis no tiene la posibilidad de determinar si la huella digital es poco o muy intradelta / extradelta.

En las figuras de la 52 a la 60 se puede observar el proceso de clasificación de un dactilograma bidelto extradelto. La imagen apenas tiene ruido y el resultado obtenido es óptimo. En la figura 52 se puede apreciar con claridad tanto el núcleo como los deltas.

Figura 52. El dactilograma que se va a analizar.

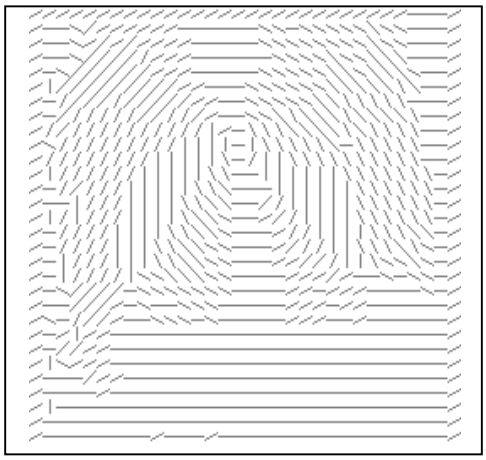


Figura 53. La imagen direccional del dactilograma.

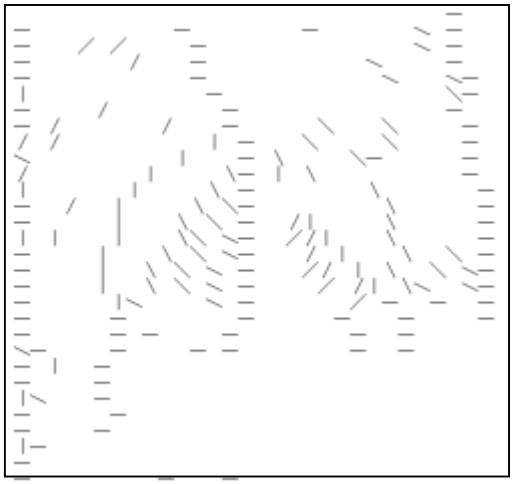


Figura 54. Selección nuclear.

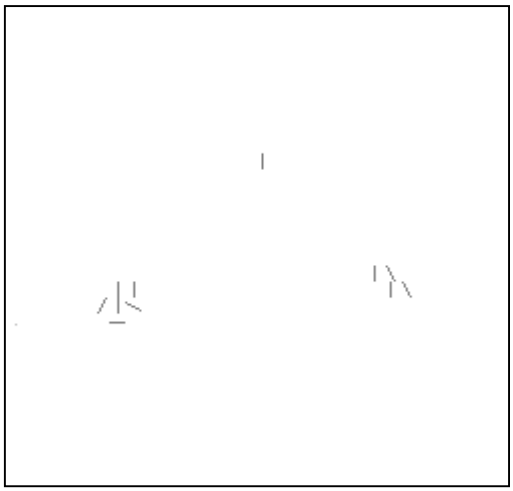


Figura 55. Eliminación déltica.

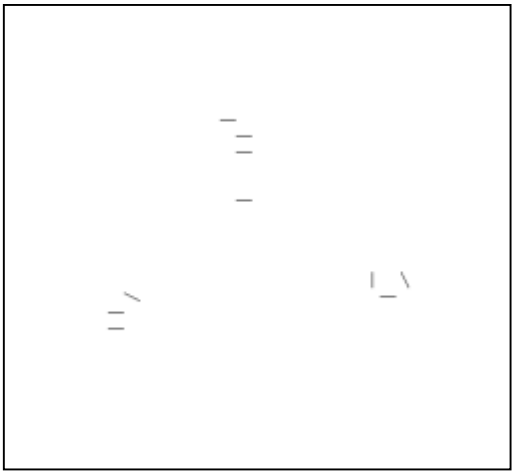


Figura 56. Eliminación nuclear.

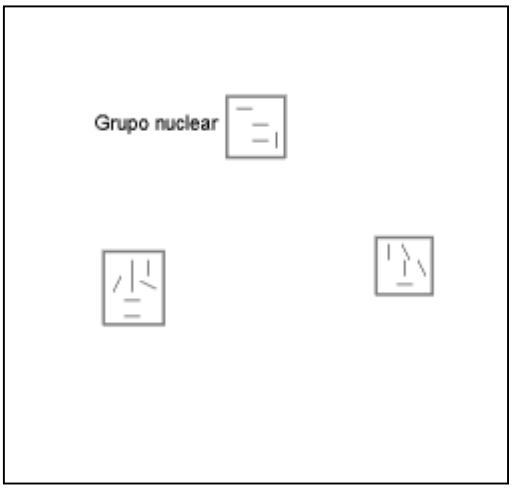


Figura 57. Agrupamiento.

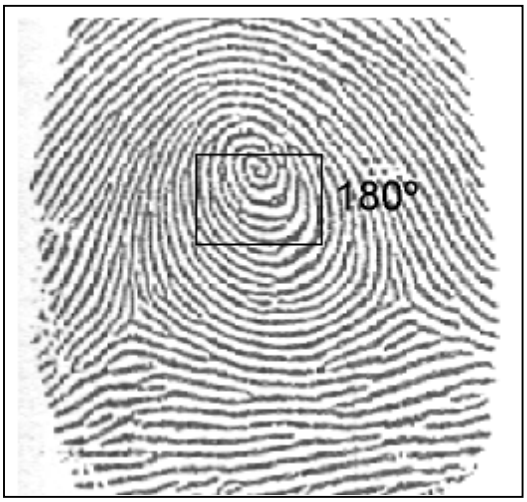


Figura 58. Localización del eje.

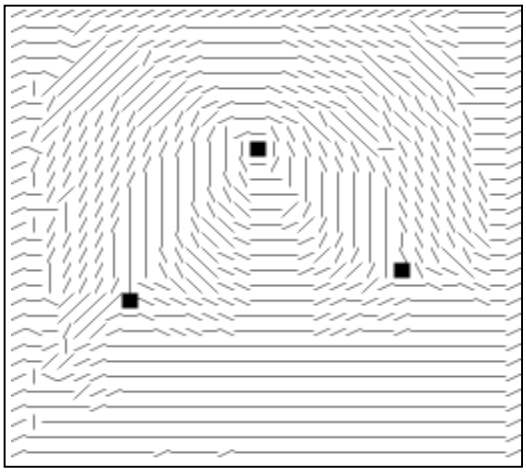


Figura 59. Localización de los puntos.

Figura 60. Resultado final. Clasificado como **bidelto extradelto**.

A continuación se ilustra un caso donde la imagen presenta algo de ruido, sin embargo no resulta un impedimento para su correcta clasificación. (ver figuras de la 61 a la 70).

Figura 61. El dactilograma a procesar.

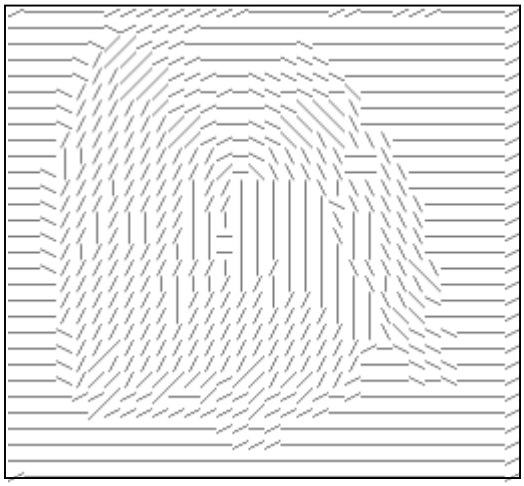


Figura 62. La imagen direccional.

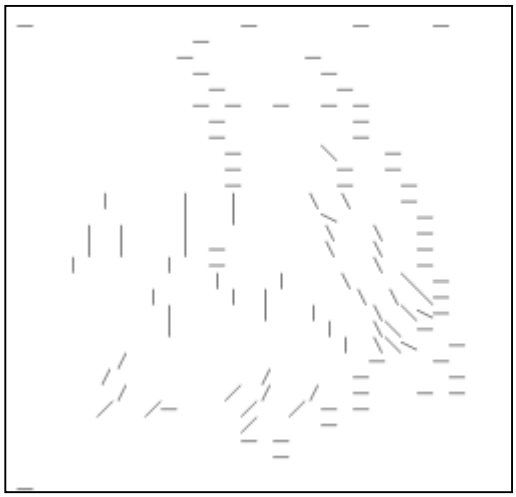


Figura 63. Selección nuclear.

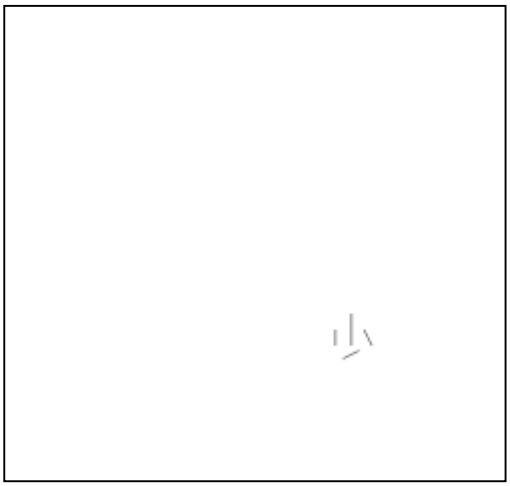


Figura 64. Eliminación déltica.

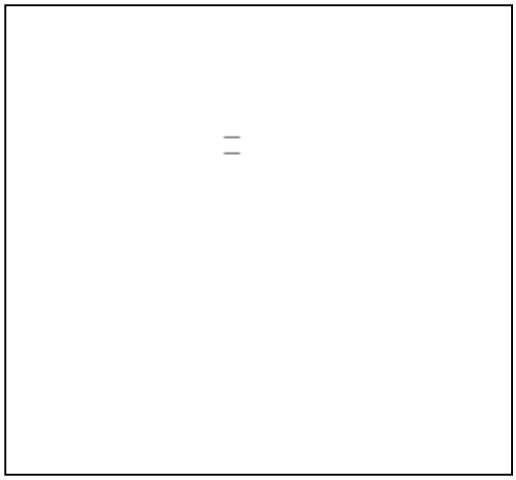


Figura 65. Eliminación nuclear.

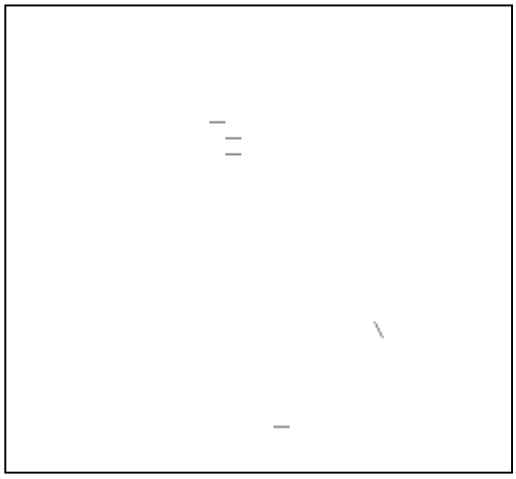


Figura 66. Detección de la curvatura.

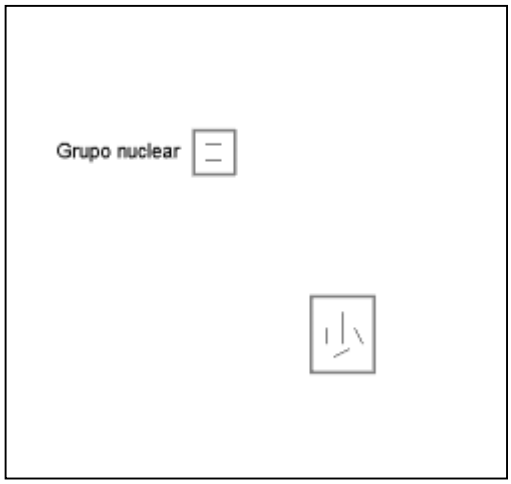


Figura 67. Agrupamiento.

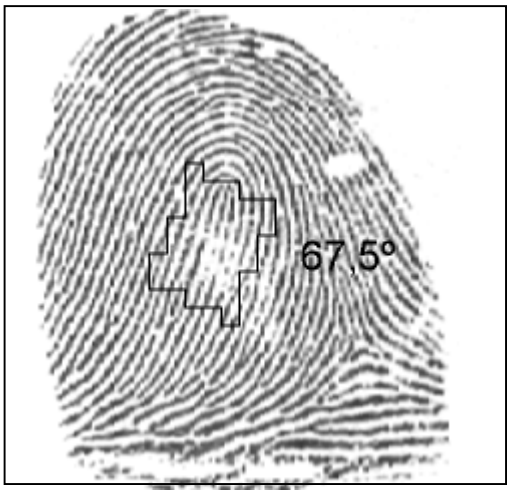


Figura 68. Localización del eje.

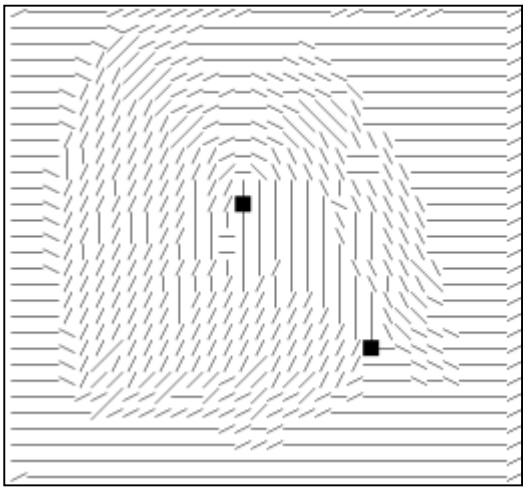


Figura 69. Localización de los puntos.

Figura 70. Resultado final. Clasificado como **dextrodelto 11.**

ANEXO 2

RESUMEN DE LOS CRITERIOS PARA LA SELECCIÓN DE TECNOLOGÍAS BIOMÉTRICAS

Criterios para la selección de los métodos biométricos

- Algoritmos correctos
- Algoritmos seguros
  - Incondicionalmente seguro
  - Computacionalmente seguro
- Buena selección de las claves
- Códigos fuertes
- Base de datos seguras
  - El administrador de la base de datos debe ser personal de confianza
  - La plantilla en la base de datos debe ser almacenada, distribuida y manejada con seguridad
- Protocolos seguros
- Redes y sistemas de distribución seguros

Criterios para la selección de los dispositivos biométricos

Operacional:

- Uso conveniente:
  - Tiempos mínimos para la inscripción, la autenticación y la verificación.
  - Acciones mínimas por parte del usuario.
  - Entrenamiento mínimo para el usuario.
  - Mínimas mediciones y almacenamiento de datos.
  - Tiempo mínimo para el reconocimiento del individuo.

- Aceptación pública:
  - Amistoso para el usuario.
  - Físicamente y legalmente robusto.
  - Seguridad para el usuario.
  - Familiar.
  - Ético.
  - Privado.
  - Socialmente no desagradable.
  - Facilidad en el uso.
  - Conforme con los estándares sociales contemporáneos.
  - Difícil de engañar
  - Baja probabilidad de ser evadido.
  - Confiabilidad y capacidad de mantenimiento.
  - Compatible.
- Unicidad (el resultado debe ser único)
- Permanencia (el identificador no debe cambiar o ser variable)
- Exclusividad (ninguna otra forma de identificación debe ser necesaria o utilizada).
- Factores humanos
  - No intrusivo (ningún contacto físico con el identificador)
  - No discriminatorio (contra: género, edad, condición física y fisiológica, profesión, características físicas impuestas).
  - Conveniente para el uso particular (ej.: la huella digital no es conveniente en los ambientes donde se requiere "manos libres").

Técnico:

- Tiempo mínimo para la autenticación.
  - Para la preparación del usuario y del sistema.
  - Para la adquisición de los bio-datos.
  - Para el proceso de concordancia (tiempo de la verificación).
  - Medición y almacenamiento.
  - Tamaño de la memoria de la plantilla.

- Nivel de tolerancia bajo.
  - Debe ser ajustable el umbral para la aceptación y el rechazo (dependiendo del nivel de seguridad requerido).
  - Bajos niveles de falsa aceptación y falso rechazo (errores tipo I y tipo II).
  - Auto adaptable.
- Flexibilidad.
- Solidez.
- Eficacia.
- Funcionamiento.
- Estándares (compatibilidad, interoperabilidad).
- Almacenabilidad (en sistemas manuales y automatizados).
- Precisión.
- Simplicidad.
- Velocidad.
- Independiente de condiciones ambientales (ruido, luz, radiación electromagnetismo, humedad, polvo, temperatura, humedad, humo).

Financiero:

- Costo de equipo.
- Costo de la instalación.
- Costo del entrenamiento.
- Esfuerzo de tiempo y del costo implicado en la puesta al día.
- Proceso requerido implicado en los sistemas informáticos para apoyar el proceso de la identificación.
- Costo de proteger el dispositivo.
- Costo de distribución y de ayuda logística.

- Costo por soporte en la administración del sistema y por suministrar un operador capacitado durante la vida útil del equipo.

Fabricación:

- Soporte técnico.
- Intercambio de datos.

ANEXO 3

TRANSFORMADA DE FOURIER

A mediados del siglo XVII, el matemático francés J. Fourier probó matemáticamente que cualquier forma de onda, independiente de su origen, es la sumatoria de ondas senosoidales de diferentes frecuencia, amplitudes y fases. Él mostró que si una forma de onda se repite periódicamente, entonces las frecuencias de los componentes senosoidales están restringidas a valores múltiplos de la frecuencia de repetición de forma de onda (Irizar,1999).

La transformada de Fourier representa una suma de ondas de formas senosoidales con diferentes amplitudes, fases y frecuencias.

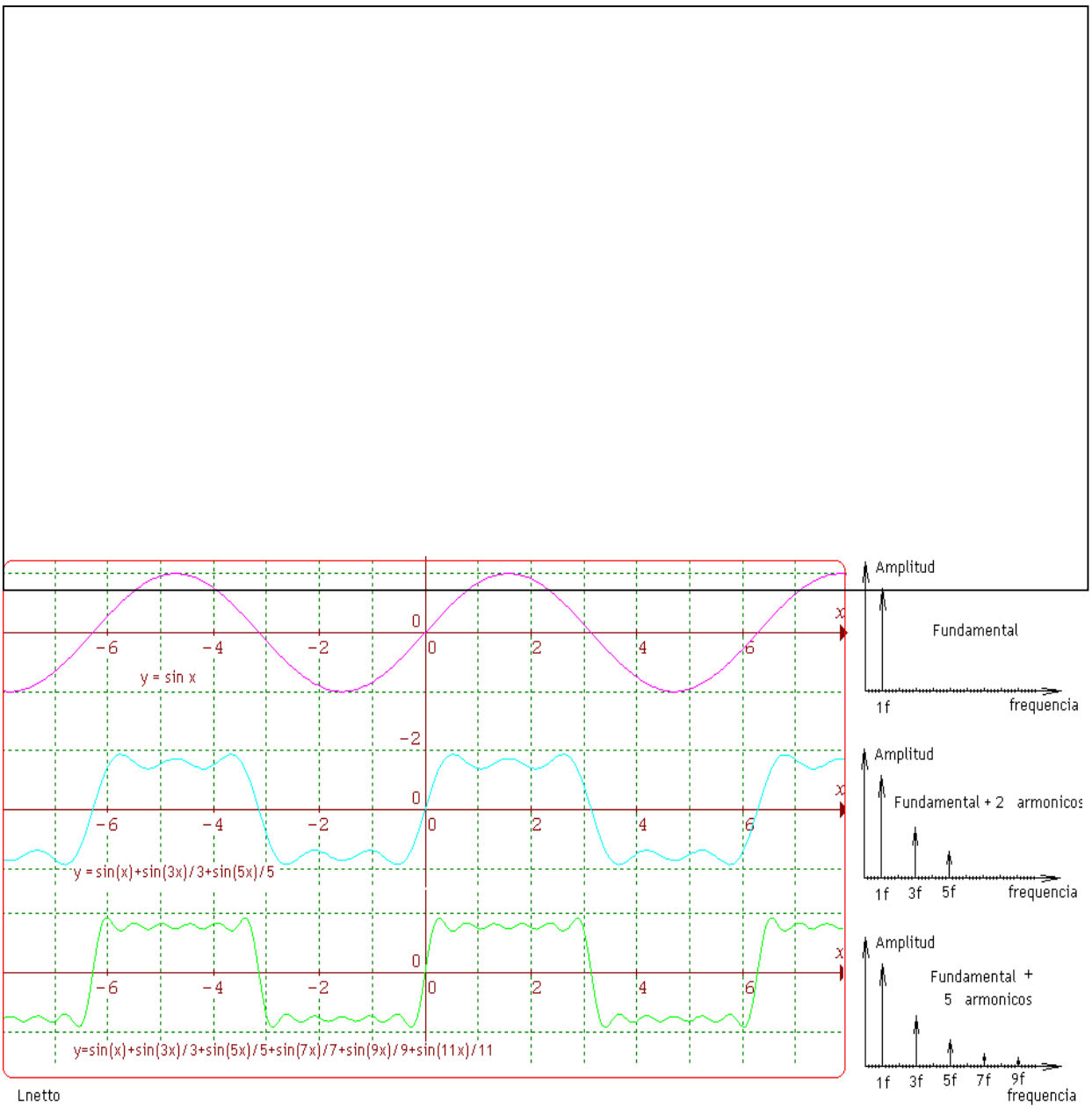


Figura 71. Transformada de Fourier

Fourier descubrió que: cualquier señal compleja puede ser descompuesta en señales senosoidales con fases y amplitudes determinadas.

$$2\pi f = \omega$$

f = **frecuencia,** t = **tiempo,** $T = 1/f$ = **periodo**

ω = **velocidad angular,** $\omega = 2\pi f$, $\omega = 2\pi/T$

$y = \text{sen}\omega t$ **Movimiento armónico simple.**

$\omega t = x$

$$y = \text{sen}\ \overset{x}{(\omega . t)} + \text{sin}\overset{3x}{(3 . \omega . t)}/3 + \text{sen}\overset{5x}{(5 . \omega . t)}/5$$

$$y = \text{sen}\ x + \text{sen}\ (3x)/3 + \text{sen}\ (5x)/5 + \text{sen}\ (7x)/7 + \ldots$$

Ecuación fundamental de movimientos armónicos de orden impar

Si a la ecuación anterior se le da valores y es graficada se podrá ver la forma de la siguiente onda:

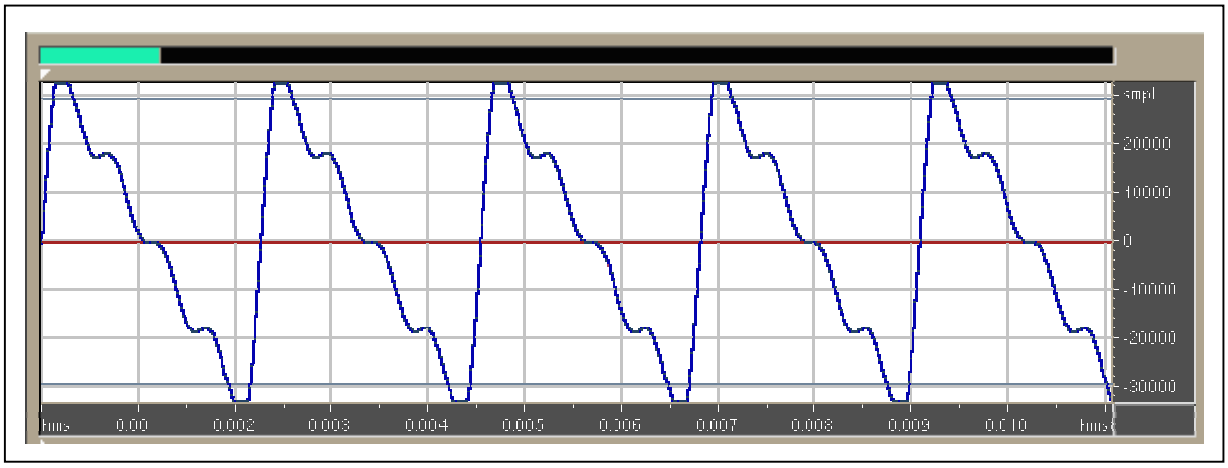


Figura 72. Onda diente de sierra

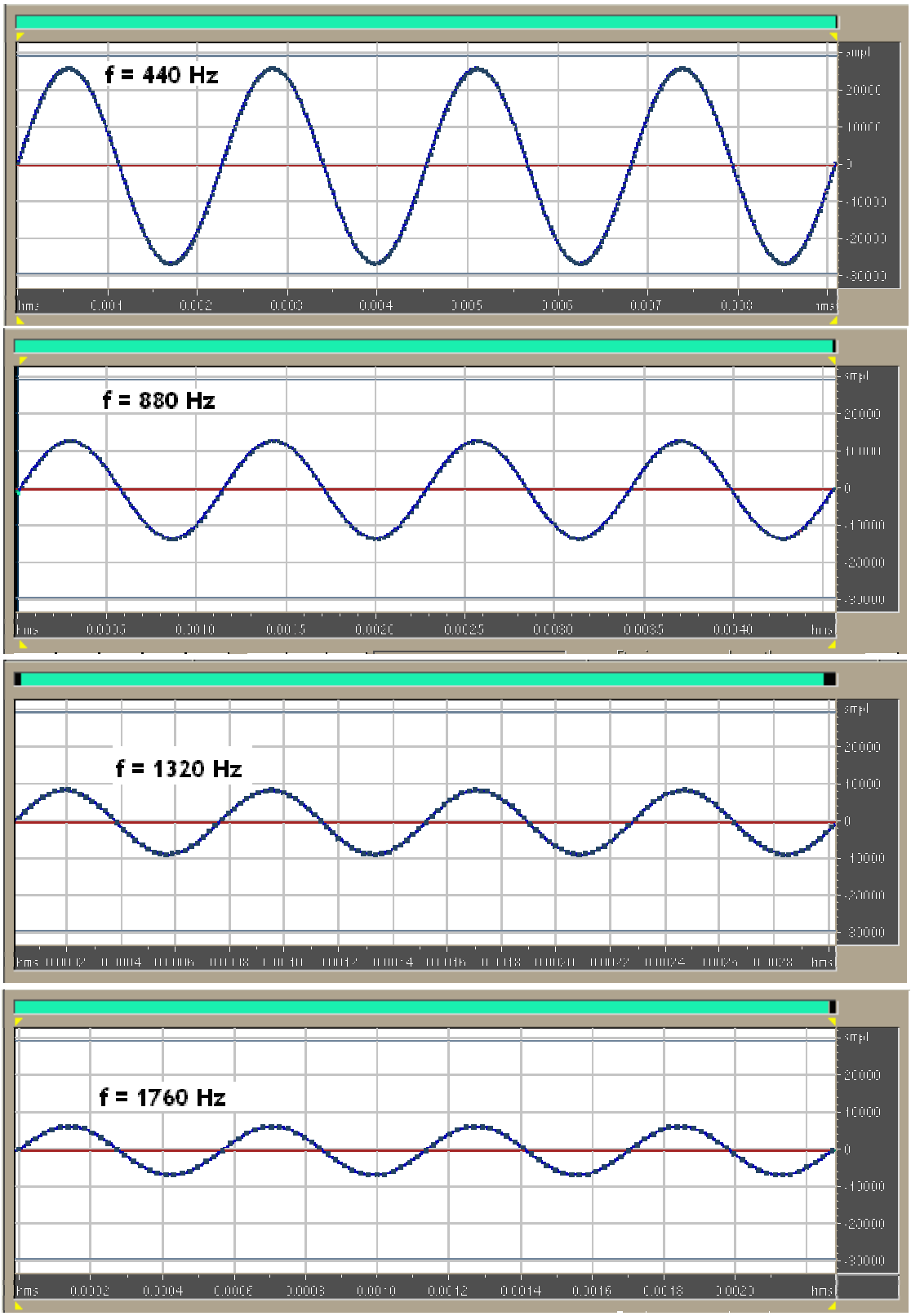


Figura 73. Componentes senosoidales de una onda diente de sierra.

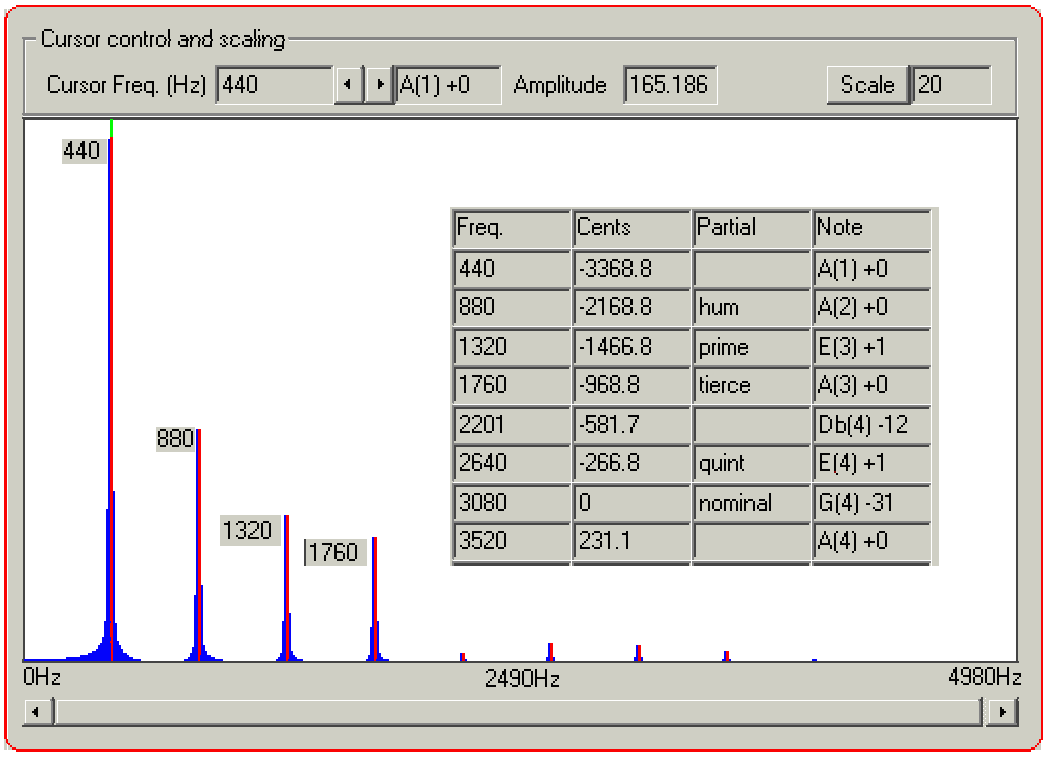


Figura 74.Análisis del espectro de frecuencia de la onda diente de sierra

Consideraciones generales sobre el patrón de la voz

- Las vocales se componen de 2 o más ondas simples, son ricas en frecuencias secundarias y contienen estructuras internas que incluyen ondas cíclicas y aciclicas.
- Las ondas acíclicas no tienen patrones repetitivos generalmente llamados ruido, forman parte de todos los fonemas sonoros, consonantes y semivocales.
- Las frecuencias y características de los patrones acíclicos proveen información importante sobre la identidad de los fonemas.
- La identidad de las consonantes también se revela por el cambio en las formantes que resultan cuando los articuladores se mueven de un fonema anterior a la consonante y de ella al siguiente fonema llamadas transiciones de formantes; éstas se analizan utilizando técnicas como la transformada rápida de Fourier (FFT) generando espectrogramas.

- La complejidad de las formas de onda de los fonemas y las constantes transiciones de un patrón a otro dificultan el análisis de los patrones utilizando las representaciones complejas de las ondas. Los patrones armónicos y de ruido se muestran con más claridad utilizando los espectrogramas de banda ancha. La localización (la distancia entre ellas) y cambio en las formantes ayudan a identificar fonemas y palabras.