BENEMERITA UNIVERSIDAD AUTONOMA DE PUEBLA

FACULTAD DE CIENCIAS DE LA COMPUTACION

"CUERPO HUMANO COMO LLAVE DE ACCESO EN LA TECNOLOGIA BIOMETRICA DEL PRESENTE Y FUTURO DE LA SOCIEDAD"

PARA OBTENER EL TITULO DE LICENCIADO EN CIENCIAS DE LA COMPUTACION

PRESENTA: DULCE MARIA DIAZ PEREZ

ASESOR: M. C. LUIS ERASMO MONTEALEGRE VÁZQUEZ

COASESOR: DR. MANUEL MARTIN ORTIZ

NOVIEMBRE, 2008

A DIOS

Le doy gracias por permitirme ver la luz de un nuevo día, desde el momento en que vi por primera vez el mundo tan perfecto que creó y así poder ser feliz en cada momento de mi existencia.

A MI MADRE

Que ha sido el sustento para poder forjar mi carrera profesional, por todo ese apoyo tan incondicional que me ha brindado y sobre todo por enseñarme que por muy difícil que sea la situación siempre se puede salir adelante. Te quiero mucho.

A MI FAMILIA

A mi esposo y a mi hija que son los grandes amores de mi vida y que por ellos lucho cada día para demostrarles que cada esfuerzo tiene una gran recompensa no les fallare, ya que los amo mucho.

A mis hermanos y demás familiares que nunca me han dejado de apoyar moralmente y que siempre están para tenderme una mano si así lo necesito mil gracias.

A LOS QUE PUDIERON HACER POSIBLE ESTA TESIS

Mi universidad el Instituto de Estudios Superiores, mi asesor M. C. Luis Erasmo Montealegre Vázquez, mi coasesor Dr. Manuel Martín Ortiz y el medio por el cual he llegado hasta acá en mi carrera profesional la BUAP.

INDICE DE CONTENIDO

CAPITULO III Metodología de Daugman (para la identificación del iris)

INTRODUCCION

Nuestros ancestros tenían métodos rudimentarios para poder identificarse, a través de señas particulares que tenían en el cuerpo; conforme fue avanzando el tiempo, se exigieron así mismos una marca personal. De esa forma se hicieron investigaciones para poder determinar patrones característicos de las personas, dando como resultado un método de identificación en forma automática: las tecnologías biométricas. En esta tesis se describe la utilidad, beneficios, desventajas, del uso de sistemas de identificación personal, para proporcionar seguridad de acceso, lo que conlleva a evitar falsificaciones de autentificación con claves habituales, además de estudiar el funcionamiento del cuerpo humano (rasgos faciales, iris, mano, forma de caminar, etc.), como llave de acceso en sistemas de identificación, así como proporcionar los posibles factores de error de los sistemas biométricos que dan fallo a la autentificación de las personas (por ejemplo los gemelos), desde una base de datos, la cual permite identificar rápidamente a personas a través de un sistema AFIS (Sistema Automático de Identificación de Huellas Dactilares), con el fin de saber si esta infringiendo la ley de su país o la de algún otro o simplemente la corroboración si es quien dice ser.

Sin embargo las opiniones de la sociedad acerca de tomar como sistema inteligente la identificación de personas, son muy encontradas por los pro y los contra que tiene, se pretende en un futuro establecerla como un requisito indispensable para registrarse en una base de datos y posteriormente ser identificados.

El objetivo de esta investigación es exponer los grandes beneficios y las utilidades de los sistemas biométricos en el sector social, para dejar atrás las claves habituales y la incertidumbre de una posible falsificación y así darles mayor seguridad a los usuarios. Mediante una recolección de todos los elementos que componen la biometría encontraremos en muchos artículos, publicaciones, documentos, etc., esencia de lo que es la biometría o en su defecto podremos

encontrar en concreto cada uno de los conceptos y las formas en que están constituidas las diferentes ramas de la biometría, y cómo funcionan a través del cuerpo humano. La biometría no sólo es una tecnología para identificar a las personas ya que hay muchos detalles detrás de todo sistema biométrico: desde los posibles errores que puede ocasionar un sistema biométrico (por ejemplo podría ser burlado con una réplica), hasta el fallo de la autentificación por tratarse de gemelos. Podremos entender con mucha facilidad en que consiste la biometría, cómo están conformadas las diferentes formas de identificación, desde las más comunes hasta las que aun no han alcanzado tanto auge en el sector social.

El Capítulo I consta de la evolución de la tecnología biométrica, así como las ventajas y desventajas que tiene en el uso de los sistemas biométricos, el Capítulo II describe a detalle en que consiste el sistema biométrico, las diferentes técnicas que se utilizan, su funcionamiento y de que ésta compuesta cada una de las características físicas del cuerpo, para la identificación de personas a grandes distancias o en diferentes circunstancias, en el Capítulo III hablaremos de como se llevó a cabo el proceso de identificación con técnicas biométricas a partir del reconocimiento del iris descrito por Tisse et al. [1]

CAPITULO I

Alcances y límites de la biometría.

1.1 Alcances de la biometría

La biometría tiene diferentes ventajas y alcances las cuales serán mencionadas a continuación.

- Mayor control de acceso físicamente [2].

- Es más segura y cómoda que los sistemas tradicionales basados en los passwords o tarjetas [3].

- Con la identificación biométrica no tiene uno que recordar alguna frase o una tarjeta con ciertas características.

- Con las bases de datos, que guardan los rasgos físicos de las personas es mucho más fácil y rápido identificar a las personas.

- La identificación verdadera de la(s) persona(s) que desea(n) hacer una transacción comercial[2].

- Posibilidades escasas de usurpación de la identidad de alguna persona.

Gracias al desarrollo de software avanzado la identificación es más exacta y viable hoy en día, en los sectores públicos o privados que tienen por objetivo una seguridad en cuanto a acceso de información.

Teniendo como llave al cuerpo humano se lucha contra el robo de identidad, fraudes bancarios, también favorece la seguridad en la información que se tiene guardada de la persona o empresa.

A lo largo de toda la vida las partes del cuerpo humano (por ejemplo la mano, la huella, el iris), nunca cambian, por lo cual se puede decir que es una llave de acceso ilimitada.

1.2 Límites de la biometría

La biometría abarca muchas ramas en cuanto a seguridad, por lo tanto llega a tener algunas limitaciones como veremos a continuación:

- Crean una falsa sensación de seguridad en la persona y no necesariamente del dato biométrico guardado, si no de sus pertenencias. Por ejemplo: el hecho de que el cliente tenga en su cuerpo la llave biométrica y pueda tener acceso a su información u objetos guardados, no quiere decir que sea el único con acceso, también lo están los encargados de los sistemas biométricos.

- La multiplicación de bases de datos biométricos.

- Las personas pueden perder derechos y libertades que tienen, en el acceso de información, ya que los encargados del sistema pueden restringirles ciertas áreas por alguna anomalía.

- Al tener tecnología biométrica a mayor exactitud y fiabilidad ésta es más costosa.

- El lector biométrico puede fallar al identificar a una persona por el aspecto físico en que éste se encuentre en el momento de querer identificarse. Podría ser que una persona va caminando pero está ebrio, la forma de caminar varía o si la persona lleva cubierta parte de la cara por alguna herida.

Las personas que tienen acceso a las bases de datos pueden hacer un mal uso de los datos de una persona y así violar su identidad alterando sus datos o eliminándolos e incluso monitorear lo que ésta haciendo en ese momento.

En el proceso de identificación, puede haber ruido en la transmisión de datos, lo cual provoca una distorsión de lo que se pretende identificar, negando

el acceso, como puede ser alguna cicatriz en la huella dactilar, o en su defecto que el lector biométrico no tenga mantenimiento frecuentemente.

Muchas ocasiones es difícil identificar gemelos, en los procesos biométricos en algunos casos la identificación no es exacta igualmente en personas con cirugías estéticas.

El contenido de las bases de datos puede ser usada con fines de extorsión por parte de las personas encargadas de los sistemas biométricos como podría ser: estudios de comportamiento de la persona sin su consentimiento, para crear perfiles sin que el cliente lo sepa.

Las personas al registrarse en una base de datos pueden dar mal sus datos personales, teniendo así problemas en un futuro.

1.3 ¿Por qué utilizar la Biometría?

La utilización de la tecnología biométrica, aplicada con sistemas biométricos, nos da una seguridad, para que las demás personas no tengan acceso a nuestra información o a un objeto que no ésta al alcance de la vista de todos por ejemplo las cajas de seguridad en bancos privados.

Es por eso que hoy en día es mejor gastar un poco más de capital, para poder así evitar fraudes de cualquier tipo, al adquirir una tecnología que ésta basada en una base de datos y un identificador biométrico.

Si esta tecnología se hubiese implementado con anterioridad, se hubieran podido evitar: robos a casas, autos, dinero, etc., así como evitar actos terroristas en el mundo, o sencillamente registrar la hora de entrada a un trabajo.

Los métodos biométricos de identificación en comparación con los métodos clásicos radican en que la persona es la "llave", la parte física del cuerpo no puede perderse ni robarse y la falsificación biométrica de alguna parte del cuerpo es muy costosa.

1.4 Antecedentes del problema

Cuando se empezó a utilizar la tecnología biométrica, no se podía contar con un sistema preciso, por lo cual muchas veces identificar a una persona resultaba problemático. En Japón un profesor de matemáticas hizo un dedo falso, pudiendo burlar lectores de huella digital, así como también en un estadio se hizo una prueba con reconocimiento de mano para ver que personas podían ser criminales y el sistema arrojo que el 10% del 100% eran criminales, por lo que se encontró que el sistema era erróneo. Conforme ha ido avanzando la tecnología biométrica se han podido ir quitando errores que anteriormente se generaban, ya que ahora en la identificación de la persona, se emplean algoritmos más precisos matemáticamente, además de apoyarse en aparatos más sofisticados, para evitar corrupción durante el proceso.

En el caso del reconocimiento de mano, llega haber problemas cuando la mano es pequeña porque el lector biométrico no logra reconocerla y por lo tanto el algoritmo no puede hacer un análisis, pudiendo ser en un futuro obsoleto por no ser para todo tipo de persona.

1.5 Problema biométrico

El gran problema con el que se encuentra la biometría, es que no es 100% seguro tiene sus ventajas y desventajas de acuerdo a la técnica biométrica que se utilice, ya que hay personas ingeniosas capaces de violar la seguridad más alta que pueda tener una institución, al hacer una copia tan exacta que el lector biométrico es burlado, (no siendo necesaria la persona que tiene acceso). En otro de los casos las personas que tienen acceso, no son prudentes en el momento de pasar por el lector biométrico y éste les niega el acceso. Adquirir una tecnología biométrica implica un costo, entre más precisa, es más cara, teniendo acceso a la tecnología instituciones de renombre y con capital económico.

CAPITULO II

Tecnología Biométrica

2.1 Biometría

2.1.1 Historia de la biometría

En el Siglo XIX se inician investigaciones con la biometría, a fin de identificar a personas por parte de la justicia, ya que las personas con ciertos rasgos físicos, pertenecían a un patrón, que determinaba que era un posible criminal, así muchos otros investigadores se enfocaron en rasgos específicos primordialmente en la investigación de huella digital.

En el Siglo XX varios países optan por la huella digital para la identificación de las personas. Así como también se empiezan a probar otros métodos de identificación, como es la voz, el iris del ojo, el reconocimiento facial, la forma de la mano, etc. En muchos de estos casos ya sin necesidad de tener un lector de recogimiento si no a través de fotos e imágenes tomadas por una cámara.

En la actualidad se han generado varios cambios; empleando diferentes características de la biometría, e incluso la mezcla de dos características en una sola, así como diferentes tipos de técnicas, para la identificación, y a un costo más accesible. El uso de identificación biométrica hoy en día, se utiliza sobre todo en los sistemas de vigilancia y control de acceso a lugares restringidos, así como en la entrada en las empresas, transacciones bancarias, voto electrónico y vía Internet, validación de firmas etc. Además también se cuentan las validaciones magnéticas y visuales.

2.1.2 Origen del uso de la biometría

La autentificación de información ya se venía haciendo desde muchos años atrás, con exactitud no se sabe el año, tampoco quien fue realmente el iniciador; lo cierto es que tampoco existía la tecnología como tal, si no que se utilizaban métodos tal vez rudimentarios pero con un gran peso, porque nos decían que esa información era auténtica, tales casos los encontramos expuestos aquí:

- Los egipcios la utilizaban, para realizar negocios y saber quienes eran los que intervenían en esas transacciones, éstos eran identificados con alguna característica física como las cicatrices, las medidas físicas, los ojos, la altura, etc.

- En la antigua Babilonia los reyes firmaban en unas tablas o tabletas con su huella antes de ser cocidas.

- Los chinos por su parte fueron los primeros en imprimir su huella dactilar sobre papel en cuestiones de negocios empresariales de sus tiempos. Así como también Bridgest dice en el libro de leyes chino de YungHwui: "Se establecía que para divorciarse de la esposa, el esposo debía dar un documento que expusiera siete razones para hacerlo. Todas las letras deberían estar escritas con su propia mano y signar el documento con sus huellas dactilares", estos son algunos de los antecedentes que se tiene de los chinos [4].

- En la Biblia también se menciona sobre las huellas dactilares en el Éxodo 13:9 "y puso un sello sobre su mano para memoria ante sus ojos", donde hace referencia a que las huellas dactilares son únicas en todos los seres humanos.[4]

- Desde el siglo XIX y hasta nuestros días se han ido utilizando los métodos biométricos en investigaciones criminalísticas siendo muy efectivos.

- En México en el artículo 1834 del Código Federal Civil, también son utilizadas como identificación en el sector rural, ya que muchas personas no saben firmar y por lo tanto se les dice que la firma es equivalente a la huella digital, este método también se utiliza en otros países. [4]

2.1.3 Evolución de la Tecnología Biométrica

En 1970 la empresa NEC junto con el FBI, empiezan a realizar estudios de los rasgos físicos del ser humano para automatizarlo a través de la biometría por algoritmos matemáticos.[5]

En 1880 el Dr. Henry Faulds Cirujano Superintendente que trabajaba en un hospital de Tokio propuso catalogar las huellas digitales porque eran únicas en las personas y nunca se alteraban a lo largo de la vida.

En 1882 en Paris, Alphonse Bertillon; jefe del departamento de fotografía creó el sistema Bertillonsystem con el cual tomaba una fotografía de las partes del cuerpo del criminal y registraban su características como son: la medida del pie, el brazo, el índice, así como la altura, y lo ancho de la cabeza, además no era lo único que registraban si no que también las cicatrices o tatuajes que el individuo presentaba, sin embargo tenía defectos ya que las medidas en otros países eran diferentes, como las conversiones de centímetros a pulgadas.

En 1888 Juan Vucetich de Argentina, utiliza las huellas de los individuos tomadas con tinta para después hacer una comparación.

En 1900 Galton/Henry de Escocia, hace un sistema de clasificación de huellas dactilares, que consiste en comparar una huella con varias para ver cual es la correcta.

En 1924 la Brigada de Investigación Criminal emplea la identificación de huella digital.

En 1936 el oftalmólogo Frank Burch sugirió utilizar los patrones del iris como identificación de la personas.

En 1965 se emplean los AFIS con una base de datos de 810000 registros, para el reconocimiento facial a través de un papel especial.

En 1989 los oftalmólogos Aran Safir y Leonard Flor crearon algoritmos de reconocimiento de iris.

En el 2000 la Brigada de Investigación Criminal instala AFIS con el fin de buscar a criminales en una base de datos con mas de 47 millones de personas, en un promedio de 2 horas se puede concluir una búsqueda.

2.2 Descripción de la tecnología biométrica.

La biometría es una rama de la matemática estadística que analiza los datos biológicos. El término se deriva de las palabras griegas "bios" de vida y "metrón" de medida, la biometría tiene muy diversos significados y englobaremos los más importantes.

> **Es un método de identificación, autenticación, comprobación automatizada y segura, del ser humano, basándose en elementos morfológicos que son inherentes a través de características fisiológicas, de comportamiento e intransferibles del ser humano.**

La biometría se basa en el análisis de datos relacionados con el individuo, y puede clasificarse en categorías como se muestra en la figura 2.2.a.

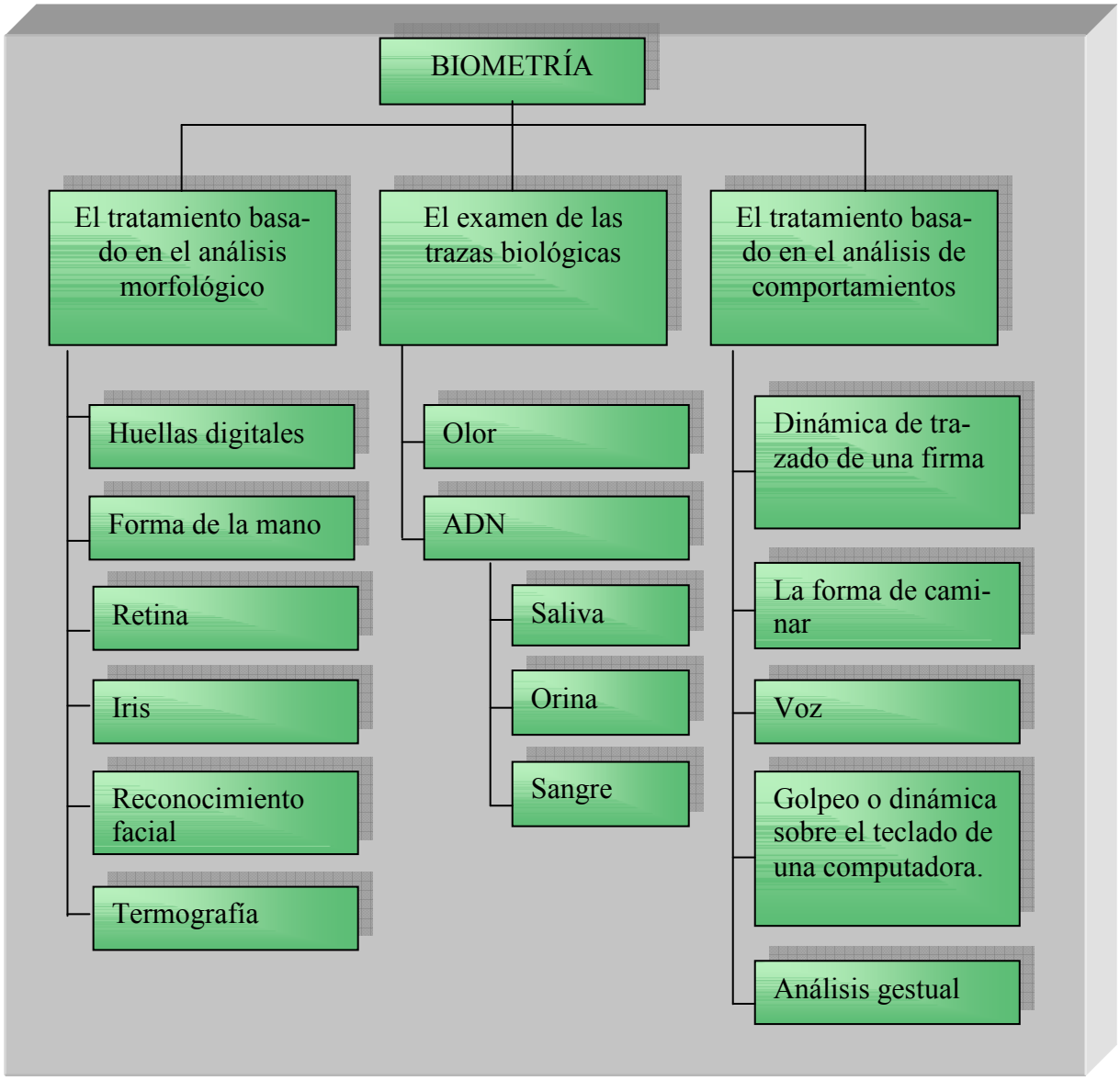

Figura 2.2.a Esquema biométrico.

La biometría se divide en 3 ramas: 1º El tratamiento basado en el análisis morfológico, que a la vez se divide en el estudio de la forma de la huella digital, la forma de la mano, retina, iris, reconocimiento facial, y termografía. 2º El examen de las trazas biológicas, que estudia el olor y el ADN comprendiendo saliva, orina y sangre. 3º El tratamiento basado en el análisis del comportamiento, el cual estudia la dinámica de trazado de una firma, la forma de caminar, la voz, el golpeo o dinámica sobre el teclado de una computadora, y el análisis gestual [3].

También existe la multi-biometria que consiste en utilizar diferentes rasgos fisiológicos en el momento de comparar la identidad de una personas en un sistema biométrico, como se muestra en el diagrama de la figura 2.2.b.

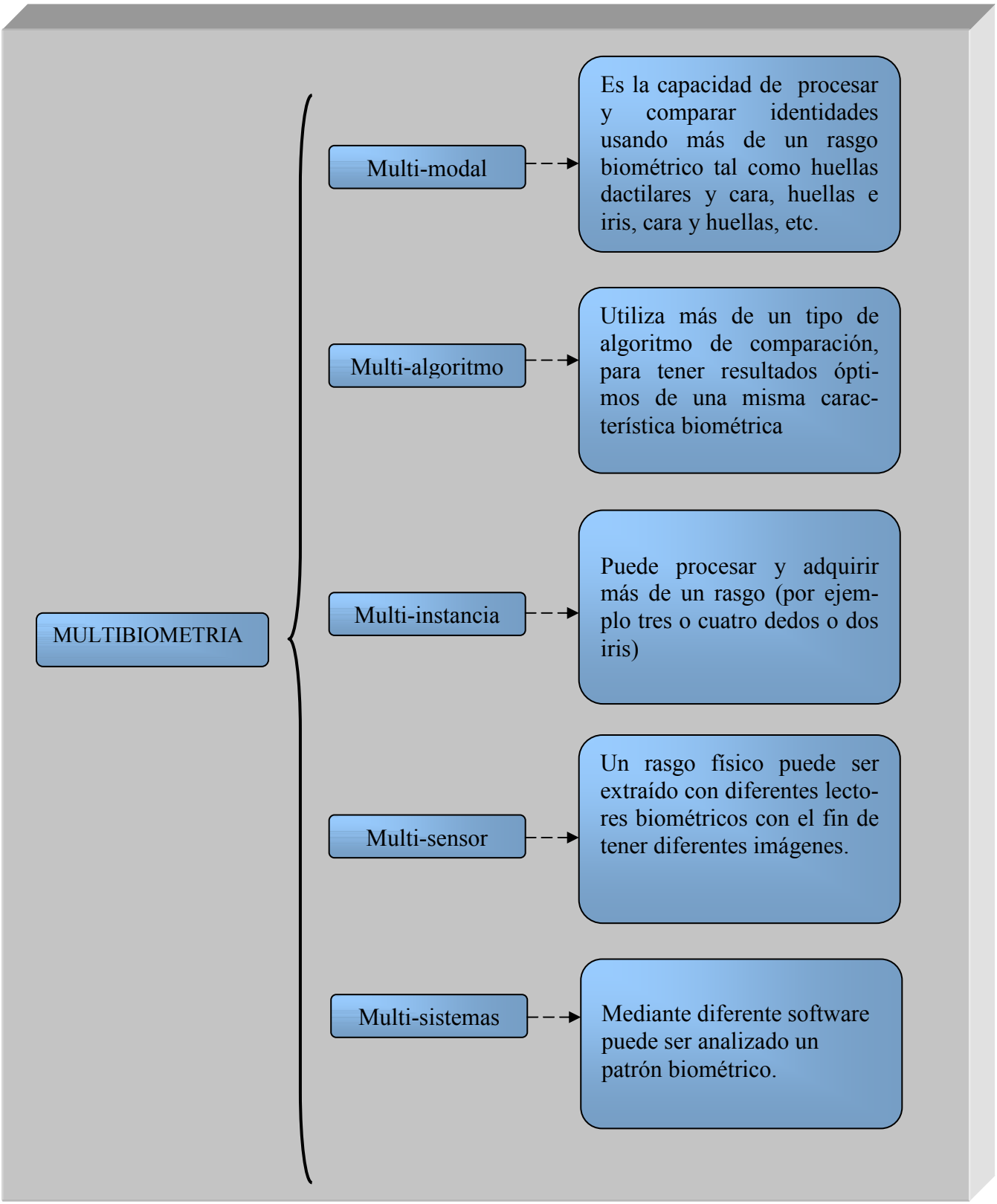

Figura 2.2.b Multi-biometria.

La multi-biometria se divide en 5, A) Multi-modal la cual procesa y compara identidades usando más de un rasgo biométrico tal como: i) huellas dactilares + cara, ii) huellas + iris, iii) iris + cara + huellas, etc. B) Multi-algoritmo, Utiliza más de un tipo de algoritmo de comparación, para tener resultados óptimos de una misma característica biométrica. C) Multi-instancia, esta Puede procesar y adquirir mas de un rasgo (por ejemplo tres o cuatro dedos o dos iris). D) Multi-sensor, este funciona examinando un rasgo físico con diferentes lectores biométricos. E) Multi-sistemas, una muestra biométrica, puede ser analizada con diferentes sistemas con el fin de ser más precisa.

Un equipo biométrico tiene las capacidades de medir, codificar, comparar, almacenar, transmitir y/ó reconocer alguna característica propia de un ser humano, con un grado de precisión y confiabilidad.

Un sistema biométrico verifica las características almacenadas de una persona contra las que pretenden ser verificadas en ese momento.

Una biometría puede calcular medidas de una muestra de referencia de la persona que se encuentra registrada en una base de datos, mediante el uso de un ecógrafo[1] y de un sistema biométrico[2]. Cualquier muestra biométrica tiene que poder recuperarse y convertirse en un formato digital cuantificable con facilidad. La solidez de la muestra se evalúa mediante la capacidad de variación del material humano básico a lo largo del tiempo como resultado de la edad, heridas, enfermedades, exposición a sustancias químicas, etc.

La muestra biométrica puede hacerse con conocimiento y participación de la persona interesada. Ésta puede también intervenir sin su conocimiento,

[1] Ecógrafo: conocido como ultrasonografÍa es una técnica diagnóstica de imágenes que utiliza ondas de sonido de alta frecuencia y una computadora para crear imágenes de vasos sanguíneos, tejidos y órganos.

[2] Los sistemas biométricos incluyen un dispositivo de captación y un software biométrico que interpreta la muestra física y la transforma en una secuencia numérica.

especialmente en la toma de huellas digitales a partir de objetos o de captura de imágenes (fotos, vídeo). [2]

Para reconocer a una persona, se procede a continuación a una segunda recogida de muestra biométrica la cual será comparada con la muestra de referencia. En caso de equivalencia, el reconocimiento es positivo.

La tecnología biométrica permite el reconocimiento y comprobación científica, de las características biológicas únicas del ser humano donde no hay ninguna otra alternativa más que el cuerpo humano, utilizando aplicaciones para validar en forma consistente la identidad de las personas con la finalidad de incrementar la seguridad y minimizar las posibilidades de fraude.

La "Biometría Informática" es la aplicación de técnicas biométricas[3], matemáticas y estadísticas sobre los rasgos físicos o conductuales de una persona, para "verificar" identidades o para "identificar" individuos en sistemas de seguridad informática.

2.2.1 Obtención biométrica

El proceso de adquirir un patrón biométrico consta de diferentes secuencias las cuales iremos describiendo a continuación:

a) Lector biométrico.- Es un sensor o sensores que permiten la extracción de una muestra, los lectores biométricos pueden ser ópticos, de campos eléctricos, ultrasónicos y térmicos.

b) Evaluación de la muestra biométrica.- Cuando se adquiere una muestra biométrica ésta es evaluada para ver si es de buena nitidez y las características son las adecuadas, para poderlas mejorar mediante algoritmos, y éstas sean aún de mejor calidad para guardarlas en una base de datos. En caso de

[3] Las técnicas biométricas se basan en medir al usuario directa o indirectamente para reconocerlo automáticamente aplicando técnicas estadísticas y de Inteligencia Artificial (lógica borrosa, redes neuronales, etc.)

que la muestra no sea buena se le pide a la persona volver a dejar su muestra para reevaluarla.

c) Comparación biométrica.- Mediante la comparación de la muestra biométrica, se permite dar acceso a la persona que desee ingresar a cierta petición, en tanto coincidan las muestras.

d) Base de datos.- La base de datos es primordial para dar acceso a una petición, ya que en ésta se encuentran tanto las muestras originales como la entrada de las nuevas muestras biométricas las cuales tienen que coincidir con las almacenadas en la base de datos. Desde las bases de datos se pueden hacer las comparaciones de forma remota en el momento en que éstas sean solicitadas.

Existen 7 características biométricas idóneas en el reconocimiento de una aplicación las cuales menciona Jain [6].

1 Universalidad: La universalidad es refiere a todo individuo al querer acceder a una aplicación biométrica, debe contar con el rasgo físico necesario sin ningún problema.

2 Singularidad: La singularidad consiste en que el rasgo dado debe ser lo suficientemente diferente del resto de los individuos que estén registrados.

3 Permanencia: La permanencia establece que los rasgos biométricos de un individuo no deben cambiar durante un período de tiempo con respecto al algoritmo de identificación de la maquina. Un rasgo que cambia de forma significativa con el tiempo no es biométricamente útil.

4 Mensurabilidad: La mensurabilidad establece que los lectores biométricos con los que se toman las muestras no deben causar molestias o incomodi-

dades a las personas para que la adquisición de las características sean más exactas.

5 Desempeño: Se refiere a que el reconocimiento de la parte física debe ser preciso al igual que los recursos biométricos, tal precisión debe cumplir las condiciones impuestas por las instituciones normativas.

6 Aceptabilidad: En la aceptabilidad las personas no tienen que presentar ningún inconveniente al momento de identificarse en un sistema biométrico.

7 Elusión: La elusión se refiere a la facilidad con la que el rasgo de una persona puede ser falsificado mediante artefactos (por ejemplo, un dedo falso) en el caso de rasgos físicos y la imitación en el caso de los rasgos de comportamiento.

2.2.2. Estándares biométricos

En todas las ramas de la comunicación e información se siguen estándares desde que éstos existen y cada día se van evaluando, calificando y aprobando; lo mismo sucedió cuando surgió la rama de la biometría, para que en el momento de procesar los datos, éstos no tuvieran dificultades al ser ocupados por una herramienta distinta con el mismo fin. Hay diferentes asociaciones que intervienen, así como distintas las características que pueden tener los sistemas y lectores biométricos que se vayan a utilizar en las diferentes áreas de un sector ya sea empresarial o social.

El principal regulador a nivel mundial de los estándares biométricos es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC) y en Estados Unidos el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el Ame-

rican National Standards Institute (ANSI) a continuación iremos mencionando algunos estándares biométricos reguladores.

INCITS M1: El Comité Internacional para los Estándares de Tecnologías de la Información(INCITS) se encarga de ver los mecanismos de seguridad, el programa de aplicaciones e interfaces, formatos de intercambio de datos, formatos comunes de archivos, la calidad de los datos, pruebas de rendimiento, entre otras. Así como tienen diferentes grupos de tareas, a) M1.2 se ocupa de las interfaces entre los componentes biométricos y sub-sistemas b)M1.3 maneja formatos de intercambio de datos cuando llegan a ser diferentes los métodos que se utilizan, c) M1.4 Se encarga de la aplicación de perfiles biométricos relativos es decir a personas que quieren hacer algún tramite en un país diferente, d) M1.5 desarrolla métricas para informar sobre el rendimiento de lectores biométricos y saber que tan eficientes son, e)M1.5 este grupo de tarea utiliza en las técnicas para no violar la privacidad de los individuos.

ISO/IECJTC1SC37: La Organización Internacional de Normalización (ISO) y La Comisión Electrotécnica Internacional (lEC) creó el conjunto de la Comisión Técnica 1 (JTCl) para ayudar en la normalización de la Información Tecnológica, la cual se organizó para crear un nuevo sub-comité: el SC37. Este subcomité tiene seis Grupos de Trabajo (GT) los cuales mencionaremos [7]:

(WG01).- El WG01 se ocupa del vocabulario biométrico y definiciones.

(WG02).- El WG02 se encarga de las interfaces técnicas biométricas.

(WG03).- El WG03 se encargan del intercambio de formato de datos biométricos.

(WG04).- El WG04 crea los perfiles de aplicación en la biometría.

(WG05).- El WG05 hace las pruebas biométricas y las presentaciones de informes.

(WG06).- El WG06 verifica los aspectos sociales de la aplicación biometría.

NISTIR 6529: También se le conoce como CBEFF (The Common Biometric Exchange File Format) se utiliza para facilitar el intercambio de datos bio-

métricos e incluso entre los diferentes componentes de un sistema biométrico (en cuanto a la estructura lógica de archivos de datos), incluye la información que se intercambia desde datos primarios (por ejemplo, la imagen de un iris), hasta datos procesados (por ejemplo, el iris amplificado). El CBEFF define un conjunto de elementos de datos que son comunes a través de múltiples tecnologías biométricos. Estos elementos de datos se sitúan en tres grandes secciones: (1) el encabezado biométrico estándar (SBH), (2) el bloque biométrico de memoria específico (BSMB), y (3) la firma del bloque (SB). CBEFF facilita la coexistencia de la Tecnología multi-biométrica en un único sistema.

ANSI X9.84: Estándar creado por el ANSI (American National Standards Institute) el cual garantiza y define las condiciones de los sistemas biométricos haciendo referencia a la recolección, gestión, transmisión y almacenamiento seguro de la información biométrica y a la seguridad del hardware asociado aunque éstos sean diferentes métodos ya que se asegura la confidencialidad, integridad y no rechazo de los datos biométricos correspondientes a las diversas modalidades.

ANSI / INCITS 358: Llamado también Bio Api Consortium, incluye especificaciones para La normalización de la interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son compatibles entre sí. La interfaz deberá ejecutar las tareas relacionadas con la recolección, la verificación y la identificación de los usuarios.

2.2.3 Huella digital

Las personas tenemos la característica de tener huellas dactilares únicas que se forman durante la 6º semana de gestación, éstas nunca cambian en el ciclo de la vida, incluso los gemelos no tienen huellas digitales iguales. El reconocimiento de la huella digital es 99.9% seguro, la persona se registra en una base de datos con sus respectivos datos personales, en el momento de comparar una huella previamente grabada en una base de datos con la original, si éstas concuerdan, la persona tiene acceso a su información o a su respectivo

resguardo en el banco de seguridad. También en los laboratorios se ésta analizando la posibilidad de que al momento de poner la huella en el lector ésta tenga pulso para evitar las posibilidad de que ésta sea una imitación o en un caso más grave sea sólo el dedo mutilado.

La huella digital tiene ciertas características y detalles en las papilas como son: arco, gancho, espiral, líneas interrumpidas (cortadas), bifurcaciones, lagos, puntos, islas, etc., como se muestra en la figura 2.2.3.a, las pequeñas arrugas que tienen están en dos formas: salientes (crestas papilares) y depresiones (surcos interpapilares), Las crestas contienen las glándulas sudoríparas, produciendo un aceite, los cuales se quedan en los surcos de la huella, al hacer contacto éstas quedan plasmadas.

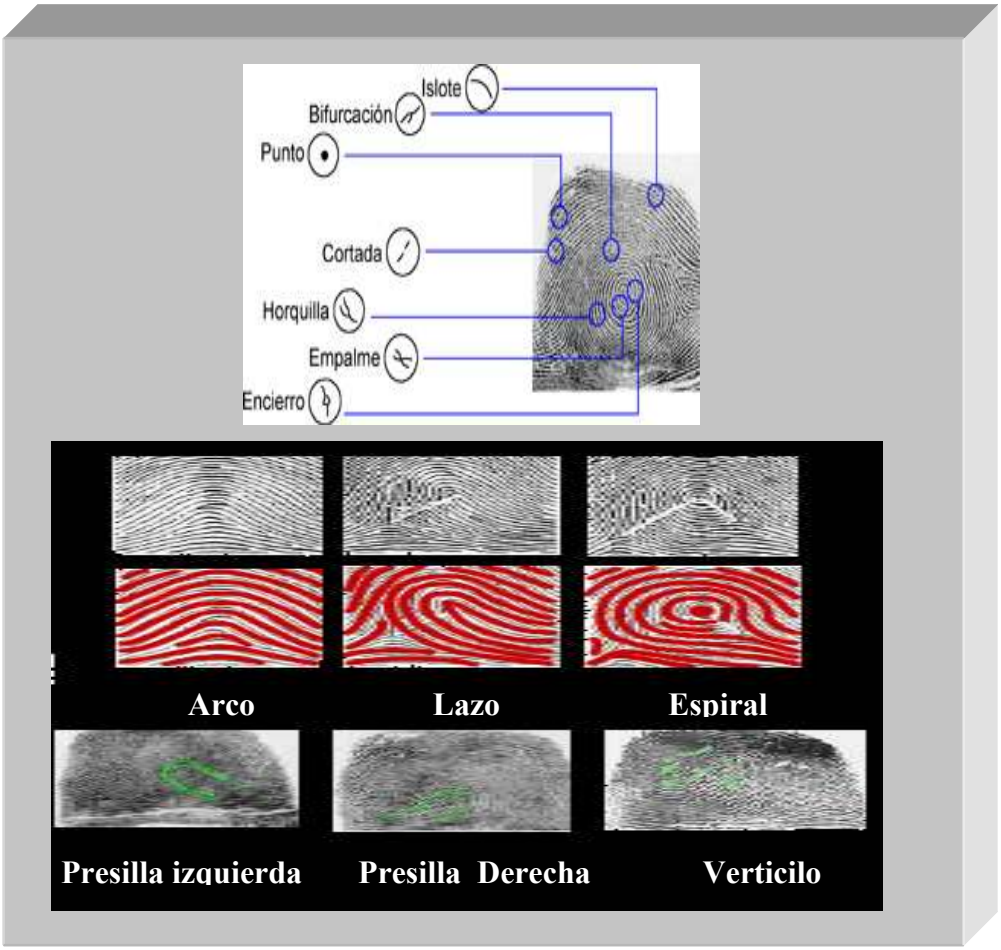

Figura 2.2.3.a Características dactilares.

La huella dactilar puede contener islote, bifurcaciones, puntos, cortadas, horquillas, empalmes, arcos, lazos, espirales presilla izquierda, presilla derecha, así

como verticilos, las cuales nos pueden ayudar a facilitar el reconocimiento de una persona.

El proceso para hacer la corroboración de la huella digital se tiene que obtener a través de un lector, un sistema que con un algoritmo extrae las minucias, y las representa en una numeración aleatoria, después crea una imagen en dos dimensiones con las característica de los puntos(x, y; en un plano cartesiano, formando ángulos dando como resultado un prisma, los cuales generan un código en unos vectores que son guardados en una base de datos; para que cuando la persona pase su huella, ésta pueda ser comparada, como se muestra en la figura 2.2.3.b.

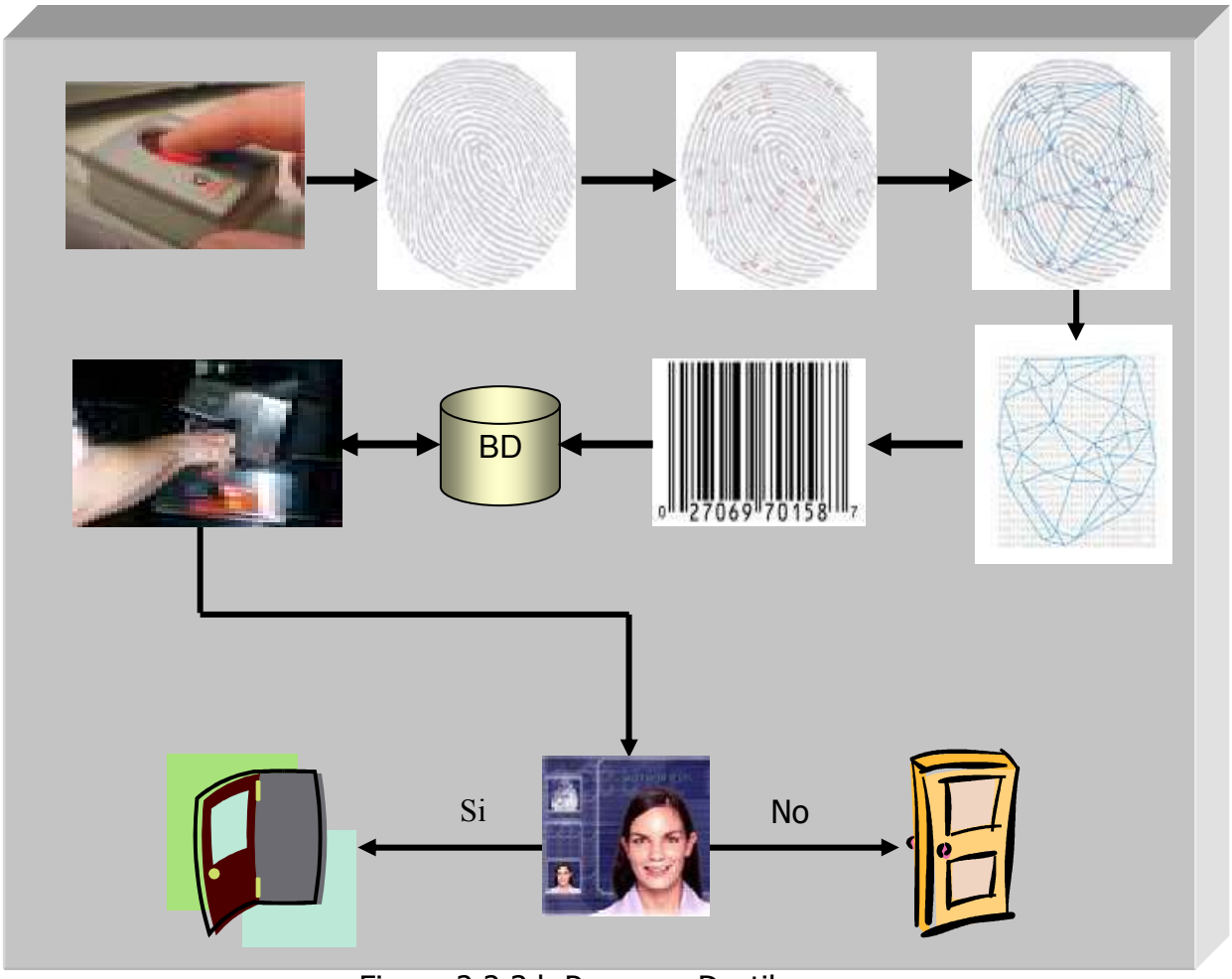

Figura 2.2.3.b Procesos Dactilar.

El proceso de identificación de huella dactilar, consiste en poner un dedo en un lector biométrico, el cual toma la muestra, genera unos puntos para unirlos y formar un prisma, el cual genera un vector de números para almacenarlos en

una base de datos, así cuando la persona quiera ser identificada, nuevamente pone su huella dactilar en el lector biométrico, y éste buscará el patrón de huella en la base de datos, para así verificar si la persona es quien dice ser, si es verídica tendrá acceso a su petición.

2.2.4 Forma de la mano

La mano tiene ciertas características como el grosor y la geometría de las venas, entre otras, así se localizan algunas de las formas pero no siempre son únicas, por lo cual se toman también imágenes de los dedos para obtener algunos datos como son longitud, altura, anchura, posición relativa, articulaciones, espesor, etc. Este tipo de sistema biométrico funciona a través de un escáner que forma una imagen tridimensional generando una serie de códigos, dicha imagen es comparada en una base datos como se muestra en la figura 2.2.4. Cabe mencionar que el lector puede no identificar la mano de alguna persona ya que la mano puede tener algún tipo de joyería, una cicatriz, un hematoma o puede tener algún factor genético lo cual impediría la identificación de la persona.

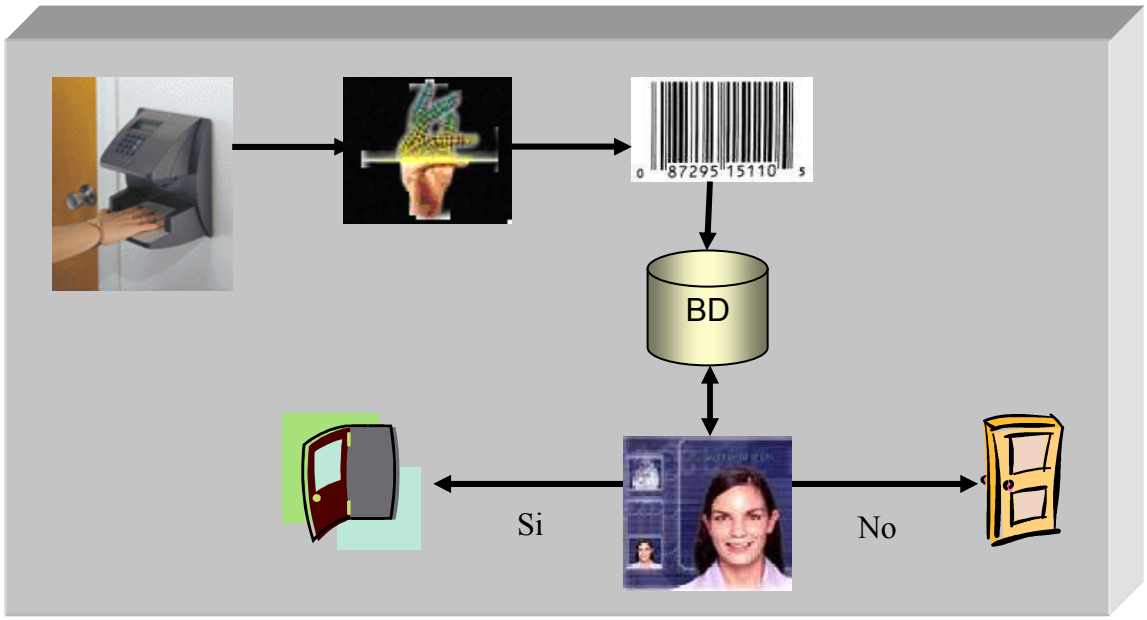

Figura 2.2.4 Proceso reconocimiento de mano.

Para registrarse o identificarse a través de la forma de la mano, se pone en un lector biométrico, el cual genera una imagen tridimensional generando un códi-

go, el cual es almacenado o verificado (según sea el caso) en una base de datos con el fin de dar acceso a la persona que hizo su petición.

2.2.5 Retina

La retina es la capa mas interna del globo ocular y es el que recibe la imagen a través de células nerviosas que captan la luz, junto con los capilares, además de estar en contacto con el humor vítreo.

Para el reconocimiento de retina, se hace un barrido de ésta a través de un acoplador óptico que emite una luz infrarroja de baja intensidad hacia la pupila del usuario, éste debe ver en un punto específico del ojo. El lector analiza las capas de los vasos sanguíneos que se encuentran atrás del ojo, para poder ver las características únicas de la retina e identificar a las personas como se muestra en la figura 2.2.5. Esta técnica es muy exacta, pero también tiene algunos inconvenientes por parte del usuario, como es mantener la mirada fija durante un tiempo determinado, si la persona guiñe el ojo tiene que volver a empezar, o para las personas que utilizan anteojos.

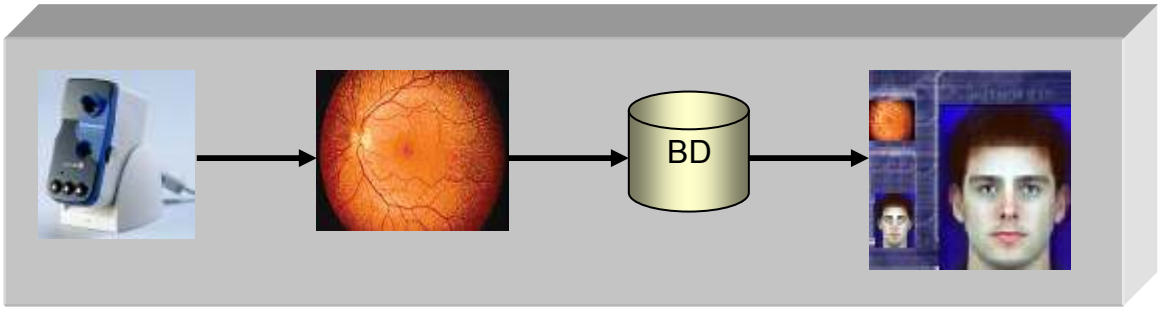

Figura 2.2.5 Reconocimiento de retina.

El proceso de reconocimiento de retina, consiste en fijar por un momento la vista en el lector biométrico, éste toma una foto de la imagen de la retina, la cual verifica en una base de datos para ver si se trata de la persona que solicito el reconocimiento.

2.2.6 Iris

El iris tiene 11 milímetros de diámetro, ésta formado por un enmarañamiento de tubos coloreados, con más de 400 características (entre criptas, sur-

cos radiales, zona pupilar, zona ciliar, bordes pigmentados, collares, anillos, fosos, pecas, corona en zig-zag como se muestra en la figura 2.2.6. El iris nunca cambia a lo largo de la vida, e incluso el iris del ojo izquierdo es diferente del derecho.

Esta técnica biométrica es mucho mas rápida que otras, y no afecta el hecho de llevar lentes de contactos o los lentes convencionales, consiste en ver a través de un lector óptico de alta resolución y el sistema va analizando sus dobleces y patrones generando una imagen, que se analiza a través de algoritmos de Daugman. La información es guardada en una base da datos, ésta tiene la ventaja de ocupar sólo 256 bytes, así la información que se ocupa es específica y no en exceso y el proceso de búsqueda es mucho más rápido cuando el usuario hace su verificación.

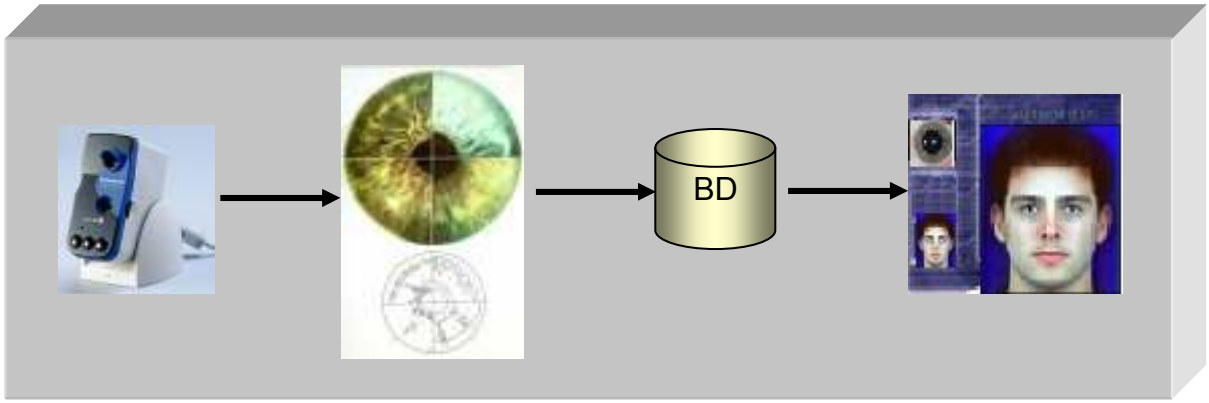

Figura 2.2.6 Reconocimiento de retina.

El reconocimiento del iris, se toma la foto de la imagen del iris de la persona a través de un lector biométrico, el sistema lo verifica en la base de datos y ésta le permite el acceso o no.

2.2.7 Reconocimiento facial

Las personas reconocemos a otra persona por medio de sus facciones del rostro, el proceso que hacemos es ver a la persona, verificamos si es conocida o no y de quien se trata, este proceso es el mismo que se aplica en los sistemas biométricos, pero para la máquina este proceso puede ser muy complejo, ya que no es lo mismo un rostro fijo, que uno con gesticulaciones. Al sis-

tema no le importa como esté el rostro o lo que lo compone (nariz, ojos, boca, orejas, etc.), ó de que raza sea la persona, debe identificarla.

La tecnología biométrica se basa en fotografías de dos o tres dimensiones. Este sistema trabaja con filtros de imágenes brillantes u oscuras, generando un algoritmo que mide distancias de puntos clave (espacio entre órbitas oculares, la nariz, la distancia entre la barbilla y la boca, la anchura de la boca, etc.), estas distancias forman una imagen tridimensional que representa el rostro, y son almacenadas en una base de datos para posteriormente ser comparadas con el original, cuando el usuario se identifica en el lector biométrico facial.

Cuando la persona se quiere identificar se pone frente al lector facial y al hacer el escaneo, puede no darles acceso por las condiciones de luz, la temperatura ambiente, la posición de la cabeza, la luz natural, etc.

2.2.8 Termografía

La termografía es la medición de la temperatura corporal, que a través de los colores emitidos, invisibles a nuestra vista, representa la temperatura corporal del ser humano.

Los seres humanos tenemos un calor corporal único, con la tecnología de termografía biométrica, se toma la muestra de una parte del calor corporal del cuerpo humano. La tecnología biométrica convierte, en tiempo real, la energía que irradia el cuerpo en forma de infrarrojo a través de una imagen termográfica. El sistema al tener la muestra, le aplica diferentes algoritmos para poder codificarlo y los guarda en un banco de datos. Cuando la persona quiere tener acceso a una determinada área, lo único que tiene que hacer es poner una parte del cuerpo (mano, cara, etc.) en el lector biométrico, y este verifica si se trata de la persona, como se muestra en la figura 2.2.8.

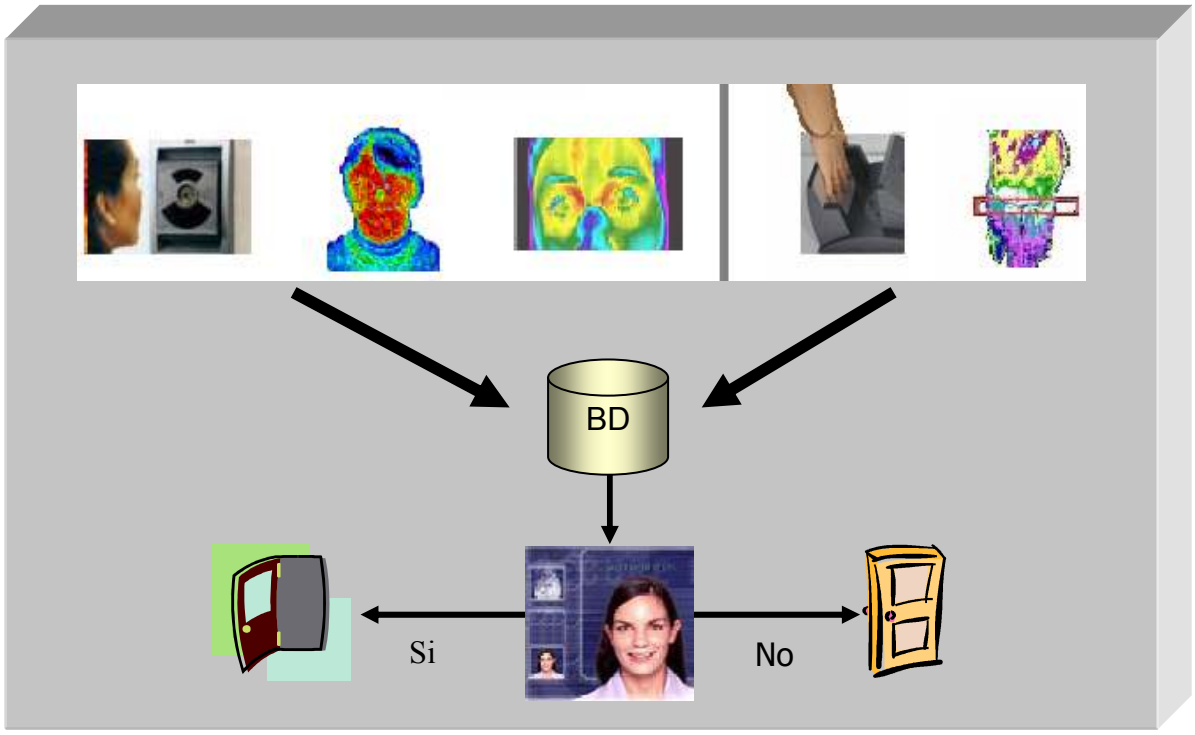

Figura 2.2.8. Termografía.

La persona se acerca al lector biométrico, y este toma el calor corporal y lo verifica en la base de datos y le da o no acceso a la persona.

2.2.9 Olor

Todas las personas tenemos un olor particular que generan ciertas moléculas del sistema inmune como son las bacterias que hay en nuestra piel y las feromonas que producimos, haciendo una formula química diferente de cada persona la cual no podemos disimular ni poniéndonos alguna colonia, o algún desodorante e incluso al bañarnos, y lo que es mas difícil, que alguien quiera duplicar ese aroma corporal ya que es único, a no ser que las personas tengan el sistema olfativo muy adiestrado, como para reconocer a una persona sin haberla visto físicamente.

Es por eso que la tecnología biométrica ha implementado un lector olfativo electrónico, que guarda las sustancias químicas volátiles que emitimos los seres humanos a través de la piel, para que después la persona se acerque al lector olfativo para que éste sea identificado, a través de la base de datos, donde se tienen guardado, los registros de la persona.

2.2.10 ADN (Saliva, orina, sangre)

El ADN es sin duda hoy la parte más estudiada por parte de la ciencia, ya que éste guarda en filamentos retorcidos (como se muestra en la figura 2.2.10) el código genético del ser humano, éste es muy delicado porque al exponerlo durante un intervalo de tiempo a una luz ultravioleta tiende a deteriorase, es por eso que la biometría también se ha encargado de estudiar el ADN con el fin de ser una llave única para las personas; el proceso que sigue es básicamente el mismo, se toma una muestra(saliva, sangre, orina, etc.) Se le aplican diferentes algoritmos para tener un código genético y se guarda en un banco de datos. Así cuando el usuario quiera ingresar ponga ya sea, una tarjeta con una muestra previa, o en algunos casos se tenga que ver por debajo de la piel. Este método no aplicaría en gemelos ya que el ADN es idéntico.

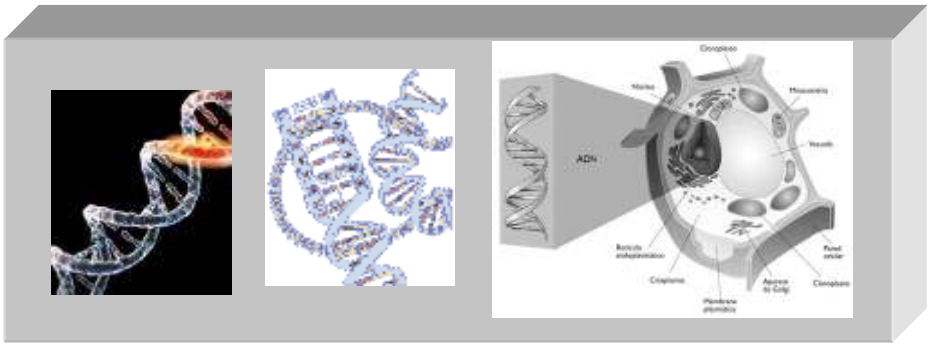

Figura 2.2.10 Reconocimiento de ADN.

2.2.11 Dinámica de trazado de una firma

Al hacer algún tipo de tramite, muchas veces se nos pide una firma para verificarla, sin embargo en algunas ocasiones no es necesario que la persona éste presente por lo cual pueden hacer usurpación de su firma. Por ejemplo cuando una empresa tiene duda acuden a personas expertas en reconocimiento de patrones de escritura, para la verificación de una firma y que ésta sea auténtica cuando se tiene duda.

Por su parte la biometría se ha encargado de hacer lectores de reconocimiento de firma (como se muestra el bolígrafo en la figura 2.2.11). Éste proceso toma en cuenta cuando la persona pone su firma en una superficie, la ve-

locidad con que se toma, la presión que ejerce el usuario, el ángulo del bolígrafo. Tomando un patrón de dicha firma, el sistema (software) biométrico la compara con una firma guarda con anterioridad en una base de datos y verifica si es auténtica ya que si la persona ésta en un estado inconveniente (ebrio o con problemas de salud como mal de Parkinson) el lector biométrico le negará el acceso.

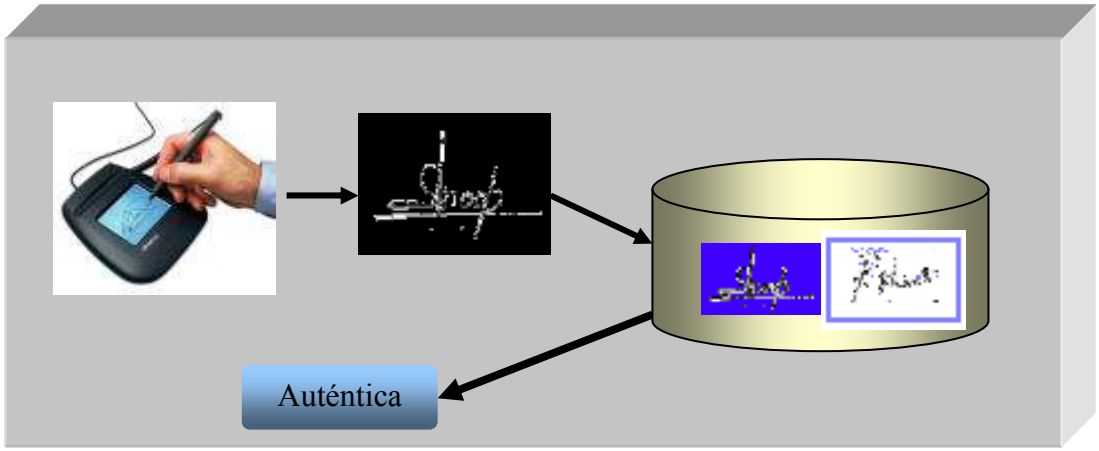

Figura 2.2.11 Dinámica de trazado de firma.

Para el reconocimiento de firma, la persona pone su firma con un bolígrafo especial, el sistema toma la impresión de la firma y la verifica en la base de datos para ver si es auténtica.

2.2.12 Forma de Caminar

Los seres humanos somos capaces de identificar o otra persona, no únicamente con verle el rostro si no también con la forma de caminar, así la persona esté a una distancia considerable de nosotros, como lo vemos cotidianamente cuando entramos a un supermercado, en las puertas automáticas, que utilizando una cámara se abren si una persona se acerca.

Este proceso es el mismo que se pretende con la tecnología biométrica, sólo que con una variación, que es analizar la forma de caminar de una persona. Los principales obstáculos que se tienen son: cuando la persona tiene cierto tipo de calzado, alguna lesión, si la persona va cansada o ebria, el suelo donde pisa no es uniforme, la ropa que porta la persona (podría variar por la soltura de la prenda)e incluso el paso del tiempo (edad). Mediante una cámara se toman diferentes fotografías y éstas son analizadas con un sistema para ver si el

patrón de movimiento corresponde al que está almacenado en una base de datos del individuo como se muestra en la figura 2.2.12. Cuando la persona se va acercando a la entrada de alguna instalación esta toma fotografías del balanceo en la forma de caminar y verifica si tiene acceso o no y de quien se trata.

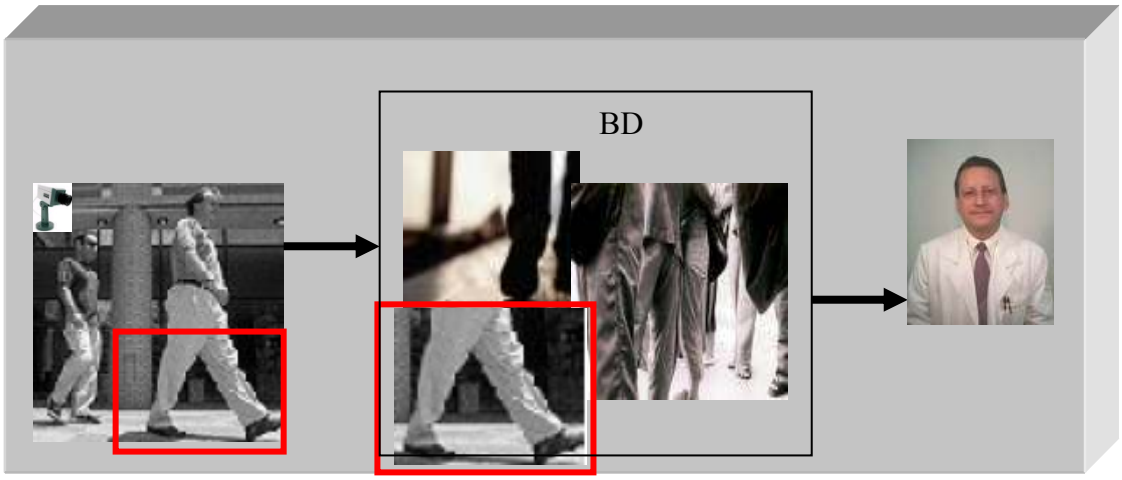

Figura 2.2.12 Forma de caminar.

Cuando una persona va llegando a una empresa tiene que registrarse, para ello se utiliza un lector biométrico, el cual le toma fotografías y las analiza, a fin de llevar un control de las personas que laboran allí y permitirles la entrada a sus departamentos.

2.2.13 Voz

La voz es otra manera más de identificación del ser humano por sus diferentes características como son el timbre de voz y grosor de voz, entre otras. En la tecnología biométrica basta con tener un micrófono (que normalmente es fácil de adquirir y no representa un gran costo) y un software adecuado en la computadora para identificar la voz de las personas mediante algún proceso como los siguientes:

- Se registra el sonido que emite la persona, el software se encarga de verificar el timbre, la intensidad y la frecuencia que tiene el patrón de voz.

- El sistema crea un modelo de la anatomía que tiene la tráquea, las cuerdas vocales y cavidades de donde se emite el sonido de la persona y almacena los patrones.
- Mediante una frase registrada en forma de texto previamente almacenado en una base de datos, el sistema siempre pedirá una frase diferente, si la frase tiene una letra de más o menos, lo rechazaría, la frase tiene que ser la misma.
- Mediante voz sobre IP, esta forma de verificar la voz se hace mediante telefonía, las características de la voz son guardadas y comprobadas por un sistema a través de algoritmos.

Cuando la persona llega al lector dice unas palabras o emite un sonido, así el sistema verifica en la base de datos si esta persona esta registrada o no. Estos sistemas tienen algunas desventajas cuando la persona esta enferma o bien otra persona con una grabación de la voz original la pasa por el lector y ésta la acepta.

2.2.14 Golpeo o dinámica sobre el teclado de una computadora

Las personas al estar escribiendo sobre el teclado de la computadora no lo hacemos de la misma forma e incluso la presión que ejercemos es diferente. Los sistemas biométricos para la dinámica del teclado se basan, en la pulsación del teclado en un intervalo de tiempo, en el momento de poner alguna contraseña. El sistema verifica en una base de datos, el tiempo en que fue tecleada la computadora además de tomar la presión con la que se ésta escribiendo y así es como reconoce que se trata de la persona que quiere entrar a un determinado archivo o información de la computadora dándole acceso.

2.2.15 Análisis Gestual

Los gestos que emitimos las personas al hablar, al responder a una seña en particular o simplemente la expresión que tenemos en la cara se puede analizar biométricamente el adquirir un sistema de reconocimiento gestual. Sin embargo es mucho más costoso que cualquier otro que exista en el mercado, ya

que requiere un estudio más profundo y la utilización de diferentes algoritmos de análisis, el proceso es muy similar al de reconocimiento facial, solo que éste no es de modo fijo si no que se puede reconocer a una persona con los sistemas a grandes distancias. Ya que se toman diferentes fotografías de las personas con gestos faciales en 2 dimensiones, éstas son analizadas para convertirlas en arreglos de los rasgos faciales y verificados en una base de datos como se muestra en la figura 2.2.15

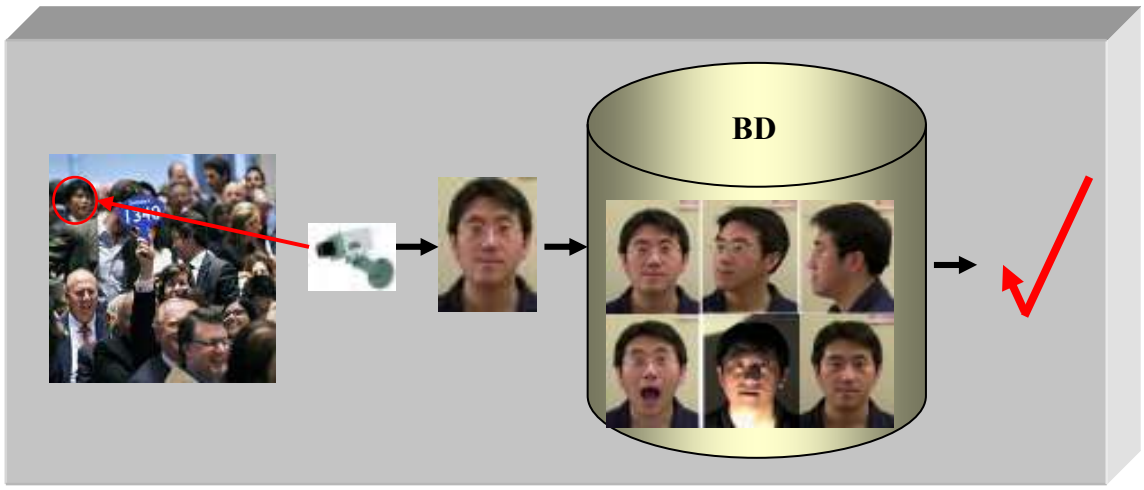

Figura 2.2.15 Reconocimiento Gestual.

El reconocimiento mediante el análisis gestual, consiste en tomar una foto de la imagen del rostro de la persona, con el lector biométrico, y se verifica que corresponda en la base de datos a la persona, si esta es verídica, tendrá acceso a la petición que haya solicitado (entrar a un edificio, etc.).

2.2.16 AFIS

AFIS (Automatic Fingerprint Identification System ó Sistema Automático de Identificación de Huellas Dactilares)

Los sistemas AFIS, sirven para consultar e identificar a personas a grandes masas, comparando sus huellas digitales, las cuales están clasificadas en impresiones dactilares o en forma de rastro latente (huella levantada en la escena de un crimen donde ésta incompleta la muestra). Esto se hace mediante un sistema biométrico compuesto por Hardware y Software de alta calidad, al capturar la imagen de la huella dactilar, este sistema biométrico tienen que

estar reconocido por las normas a nivel internacional del FBI, CSL, ANSI y NIST, como se muestra en la figura 2.2.16

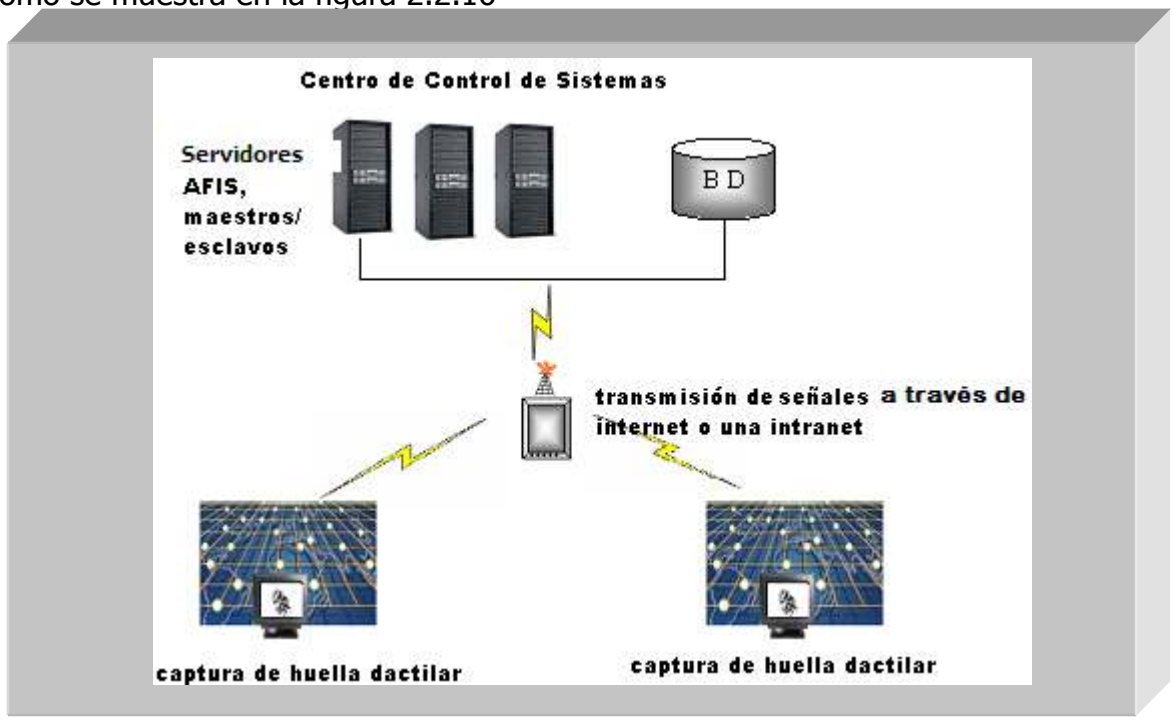

Figura 2.2.16 Método de identificación de AFIS

Consiste en tomar la huella dactilar a través de un lector de huella digital, la manda a través del internet o una intranet específica al centro de control de sistemas, donde el servidor maestro hace una comparación en la base de datos a través de los servidores esclavos, para así determinar a quien corresponde el patrón.

Existen 2 modalidades de AFIS, AFIS CIVIL Y AFIS CRIMINAL, las cuales describiremos a continuación.

AFIS CIVIL

Toda persona tiene una identificación ante la sociedad, a través de una credencial o un documento que lo avale, la cual en muchas ocasiones resulta ser insegura; en los AFIS civiles, se trata de no nada más tener una identificación si no también estar registrado en una base de datos a través de la captura de las dos huellas dactilares de los dos índices de la persona, y siguiendo el proceso de almacenamiento de huella dactilar, con el fin de evitar fraude de identidad o usurpación de identidad.

Normalmente se utilizan en los siguientes casos:

- Control de acceso de entrada en agencias.
- Documentos que acrediten la identidad de la persona.
- Procesos electorales.
- Actos jurídicos y notariales.
- En los aeropuertos y control de fronteras con inmigrantes.
- Entidades financieras.
- Acceso a prestaciones asistenciales.

El proceso que se sigue para identificar a una persona mediante huella digital, es cuando la computadora local se conecta a una red WAN, (internet),y a su vez a la red WAN se conecta a una red satelital, etc., para acceder a las bases de datos remota; y verificar si se trata de la persona que se quiere identificar.

AFIS CRIMINAL

Los AFIS en la forma de uso criminal son utilizados normalmente en el sector policiaco, criminalista, la policía fronteriza, en áreas militares, departamento de justicia, servicios secretos de inteligencia de algunos países, con el fin de luchar contra el crimen.

Los sistemas AFIS permiten realizar búsquedas como se muestra en los siguientes casos:

- Búsqueda: La búsqueda identifica a personas fichadas.
- Búsqueda Decadactilar-Latente: La búsqueda decadactilar-latente se encarga de imputar delitos a personas detenidas.
- Búsqueda Latente-Decadactilar: La búsqueda latente-decadactilar puede identificar al autor de un delito.
- Búsqueda Latente-Latente: La búsqueda latente-latente se encarga de identifica al posible autor de un delito, el sistema permite atribuirle otros delitos cometidos con anterioridad de donde se obtuvo su huella latente.

Los delincuentes pueden ser juzgadas tan sólo en base a sus huellas dactilares dejadas e identificadas si se encuentran rastros latentes en una escena de crimen.

Una huella latente puede ser una fracción ínfima de una huella dactilar, de la cual generalmente el perito no conoce a que dedo pertenece, ni su orientación, ni su centro, ni ningún otro dato que reduzca el universo de búsqueda (sexo del dueño, color de piel, etc.).

2.3 Lectores biométricos

Los lectores biométricos son muchos con diferentes diseños y sirven para un tipo de reconocimiento ya establecido; el software es lo que los hace funcionar, estos pueden variar en tamaño y precio. A continuación en la figura 3.1, se muestran la forma de como se comportan algunos lectores biométricos y en la figura 3.2 los lectores que se pueden encontrar en el mercado.

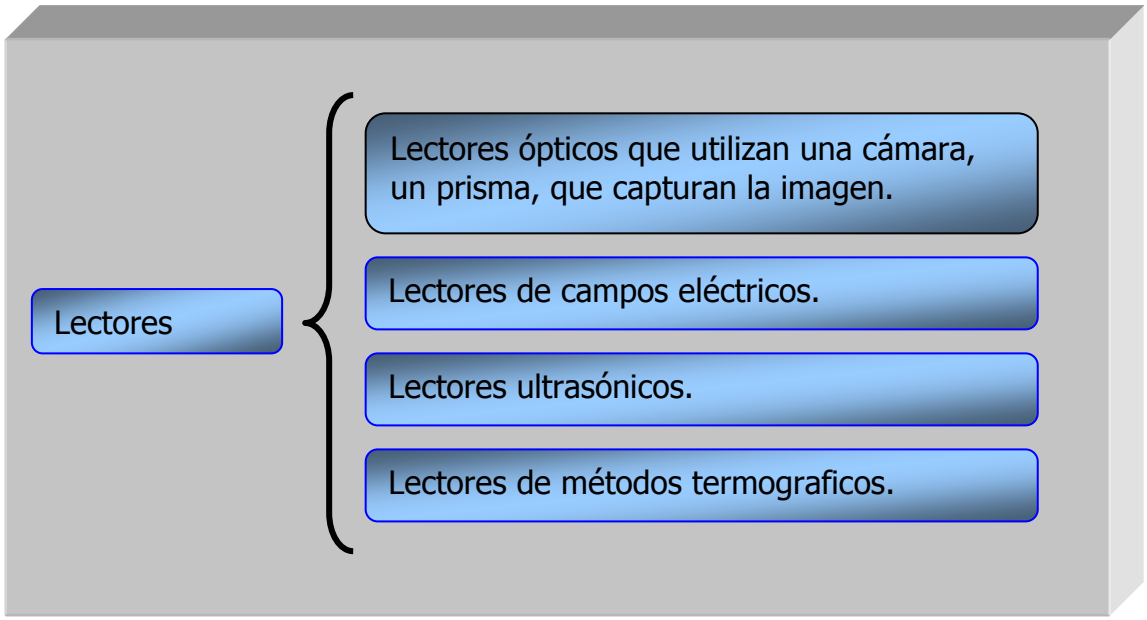

Figura 3.1 Lectores.

Los lectores pueden ser ópticos, de campos eléctricos, ultrasónicos y térmicos.

Figura 3.2 Lectores biométricos.

Los lectores biométricos son de diferentes tipos y modelos, pero todos toman fotografía para identificar a las personas, estos pueden ser lectores de huella dactilar, lector de iris o retina, lectores de la forma de la mano, lectores de firma, lectores de cámaras para termografía, cámaras para tomar imágenes faciales o la forma de caminar, lectores de voz, y bolígrafos biométricos.

2.4 Biometría empresarial

En el aeropuerto holandés de Schiphol se utilizó el reconocimiento de iris para las tripulaciones de los aviones durante un corto periodo.

En Emiratos Árabes, los pasajeros deben fotografiar su iris para cruzar la frontera; un sistema que se emplea para impedir que oculten su identidad los cerca de 420,000 inmigrantes que han sido expulsados anteriormente del país y

de los que se guarda una imagen de sus ojos en una base de datos. En cambio, en el aeropuerto Israelí de Ben Gurion se utiliza la estructura de la mano como factor biométrico, pero para identificar de forma rápida a los viajeros frecuentes que, por ello, se benefician de diversos privilegios. El método de la mano empieza también a ser muy usado para verificar la entrada y la salida de cada empleado en su trabajo, precisamente por su sencillez y eficacia.[8]

En la empresa Codorniú de Barcelona las personas tienen que identificarse a través de un lector de mano poder ingresar, y compararla con una base de datos que tiene registrado su patrón biométrico [9].

En la empresa de telecomunicaciones I+D los empleados deben pasar por un lector de geometría de mano para tener acceso al comedor [9].

En Disney World las personas que tienen pase por varios días se tienen que identificar biométricamente con la huella digital para que ninguna otra persona haga uso de su pase [10].

En el banco de seguridad de la Caixa, para que el robot pueda llevarle la caja de seguridad al cliente en la habitación en que se encuentra, la persona debe identificarse a través de la geometría de su mano en un lector biométrico [9].

En Nueva York, los empleados de la empresa American Express para poder tener ingreso deben pasar por un lector de huella digital para que puedan tener acceso al inmueble.

En los aeropuertos de Australia al momento que accede una persona en el aeropuerto es registrada a través de su rostro.

En Estados Unidos, Inglaterra, Chile, México y Colombia en algunas operaciones bancarias piden corroboración de las personas en cuestión, a través de huellas dactilares [11].

En las elecciones del 2004 en Venezuela las personas que llegaban a emitir su voto se registraban en una computadora mediante un lector de huella dactilar, y el sistema se conectaba a una base de datos, si esta persona tenía derecho a ejercer su voto se prendía una luz verde de lo contrario no podía acceder a ejercer su voto, fue implementado para evitar que un ciudadano votara 2 veces.

En Inglaterra en la primaria Wiltshire los alumnos registran su entrada a clases si no asisten a clases el sistema notifica a sus padres a través de un mensaje por celular.

CAPITULO III

Metodología de Daugman

(Para la identificación del iris)

En este capítulo encontraremos como se llevo a cabo el proceso de identificación con técnicas biométricas que ocuparon Tisse et al. [1], para el reconocimiento del iris.

3.1 Localización del iris

El primer paso consiste en la localización de los límites internos y externos del iris. El sistema de Daugman, utiliza operadores integro diferenciales (E1) para detectar el centro, el diámetro del iris y la pupila respectivamente. Estos operadores exploran la geometría circular del iris o la pupila. El sclera[4] es siempre más ligero que el iris y generalmente es más oscuro la pupila que el iris es cuando el ojo esta sano.

$$\max(r, x0, y0) = \left\{ \frac{\partial}{\partial r} \int_{0}^{2\Pi} I(r^* \cos\theta + x0, r^* \sin\theta + y0) \right. \qquad \text{E1}$$

Donde (*x0, y0*) denotan el centro potencial del límite circular buscado, y *r* es el radio.

Usando código optimizado, el tiempo de cómputo total para la detección y la localización del iris con una precisión de un solo pixel (a partir de una imagen de 640 * 480 pixeles) es de aproximadamente 250 milisegundos. Sin embargo parece que los operadores integro-diferenciales son sensibles al espectacular punto de reflexión de la luz artificial no-difusa que apunta en la dirección del centro del ojo del usuario Figura 3.1

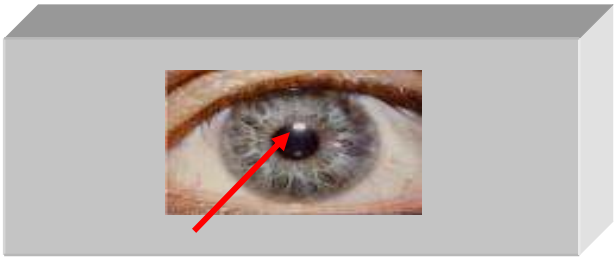

Figura 3.1 Reflejo de la pupila en el ojo.

Se toma la imagen y si ésta tiene un reflejo, se le aplican algoritmos para eliminar el reflejo para que la imagen sea pura.

[4] La parte blanca del ojo, que cubre el ojo ocular.

Los operadores integro-diferenciales se utilizan para eliminar los defectos en la imagen del ojo debido a la luz ambiental. Siempre que este punto aparezca en la pupila cerca de la frontera del iris, la detección del límite interior del iris falla.

Por lo tanto, se introduce una estrategia de detección basada en la combinación de los operadores integro-diferenciales con la transformada de Hough. Consiste en primer lugar en una técnica de cálculo del borde para aproximar la posición del ojo en la imagen global (centro de la pupila), y en segundo lugar se aplica el operador integro-diferencial para buscar con mayor precisión el límite de la pupila, el centro del iris y el límite del iris. En realidad la estrategia utiliza la transformada de Hough de descomposición de gradiente, que es una astuta variante aplicada a la detección de la forma circular.

De la ecuación del círculo $(x-x_0)^2+(y-y_0)^2=r^2, r$ donde r es el radio, expresamos las coordenadas del centro (x_0, y_0) en función de los 2 primeros gradientes de primer orden *(*G_x a lo largo del eje *x,* G_y a lo largo del eje *y)* como sigue:

$$x0 = x \pm \frac{r}{\sqrt{1+\frac{Gy^2}{Gx^2}}} \qquad y0 = x \pm \frac{r}{\sqrt{1+\frac{Gx^2}{Gy^2}}} \qquad \text{E2}$$

Donde x_0 y y_0, son acumuladores de lo ejes con respecto al radio inclinado.

Los gradientes G_x y G_x son ambos computados durante el recorrido único de la imagen del ojo. Así el problema se reduce incrementar el número de ocurrencias para cada centro supuesto a través de dos acumuladores *(*X_0 en *x,* Y_0 en *y*), y determinar el punto $(X_{0,} Y_0)$ de la imagen donde aparece un máximo en los acumuladores.

$$X_0(x_0) = \sum_x \sum_y \sum_{r-r_{\sin}}^{r_{\sin}} nbre.occurences.x_0$$

$$Y_0(y_0) = \sum_x \sum_y \sum_{r-r_{\sin}}^{r_{\sin}} nbre.occurences.y_0 \qquad \text{E3}$$

El acumulador x_0 con respecto al eje x_0 es igual a la sumatoria de cada eje y del radio menos el radio de seno hasta el radio de seno.

Considerando únicamente los componentes del gradiente superior en un umbral mínimo (definido experimentalmente) permite reducir el tiempo de cómputo. Tomar los signos de los gradientes en consideración desempeña un papel importante para excluir centros potenciales que tengan las coordenadas fuera de la imagen del ojo.

3.2 Transformación del iris en forma cartesiana a referencia polar

Localizar el iris en la imagen delinea la zona circular de análisis del iris a través de sus propios límites internos y externos (como se muestra en la Figura 3.2)

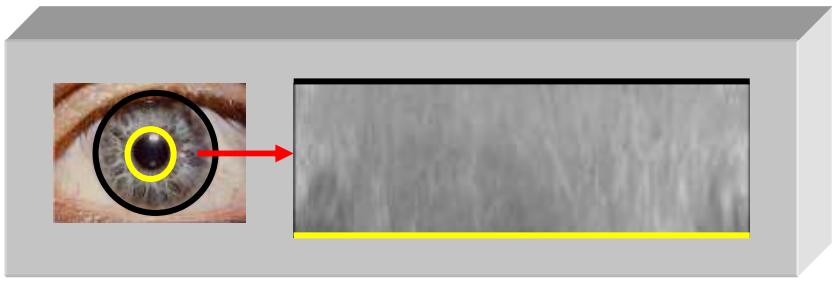

Figura 3.2 Representación rectangular del iris.

La transformada cartesiana a referencia polar sugerida por J. Daugman autoriza la representación rectangular equivalente de la zona del interés como se mostró en la figura 3.2. De esta manera se compensa el estiramiento de la textura del iris, conforme la pupila cambia de tamaño, y revelamos la información de la frecuencia contenida en la textura circular para facilitar futuras extracciones de características. El parámetro $\theta(\theta \in [0;2\pi]$ y el parámetro sin dimensiones ρ (ρ $\in [0;1])$ describen el sistema de coordenadas polares. Así las siguientes ecuaciones implementan la función $I(x(\rho,\theta), y(\rho,\theta)) \rightarrow I(\rho,\theta)$:

$$\begin{cases} x(\rho,\theta) = (1-\rho)^* x_\rho(\theta) + \rho^* x_i(\theta) \\ y(\rho,\theta) = (1-\rho)^* y_\rho(\theta) + \rho^* y_i(\theta) \end{cases} \quad \text{E4}$$

Con

$$\begin{cases} x_\rho(\theta) = x_{\rho 0}(\theta) + r_\rho{}^* \cos(\theta) \\ y_\rho(\theta) = y_{\rho 0}(\theta) + r_\rho{}^* \sin(\theta) \end{cases} \quad \text{E5}$$

$$\begin{cases} x_i(\theta) = x_{i0}(\theta) + r_i{}^* \cos(\theta) \\ y_i(\theta) = y_{i0}(\theta) + r_i{}^* \sin(\theta) \end{cases} \quad \text{E6}$$

Donde r_p y r_i representan el radio de la pupila y el radio del iris respectivamente, mientras que $(x_p(\theta), y_p, (\theta))$ y $(x_i, (\theta), y_i(\theta))$ son las coordenadas de los límites pupilares y límbicas en la dirección θ.

Las zonas de frontera (iris /pupila e iris /sclera) son truncadas para evitar ruido en la representación rectangular del iris por otros patrones no incluidos en la textura del iris y se llega a lo siguiente:

- la pupila no es perfectamente circular.
- la detección del límite externo del iris, a menudo no es bien definida debido al uso de lentes de contacto.

3.3 Instrumento de recolección

3.3.1 Extracción local de la muestra

Las características del iris se localizan basándose en el sistema de coordenadas polares. Los filtros complejos de pasa-banda 2-D de Gabor, que ofrecen la mejor resolución de la frecuencia-espacial en el caso de dos dimensiones, para extraer la información de la textura de las imágenes del iris. Como resultado de la filtración de diversas frecuencias y en posiciones particulares en el sistema coordenado polar, se calculan una serie de valores complejos a través de convolución. El signo de las partes reales e imaginarias de las proyecciones de la cuadratura de la imagen, de estas regiones específicas del iris realizan una cuantificación de fase de la señal local de la textura. El tiempo requerido para computar un código de iris completo, una vez que ha sido localizado el iris de-

ntro de la imagen, toma cerca de 100 milisegundos. Es importante observar que, debido a correlaciones radiales entre diversos patrones del iris, existe una dependencia entre los bits extraídos en códigos del iris. El estudio del número de grados de libertad indica, en el sistema del Daugman, una reducción de la capacidad de la información del código del iris por un factor de 4.05 a partir de 2.048 bits hasta aproximadamente 506 bits.

3.3.2 Frecuencia obtenida

La fase instantánea se obtiene construyendo la señal analítica, combinando la señal original y su transformada de Hilbert. Para cualquier señal real x (t), se puede formular la señal compleja x, z_x (t) como sigue:

$$z_x(t) = x(t) + j..H\{x(t)\} \qquad \text{E7}$$

La señal $z_x(t)$ es cambiada por la señal analítica donde $H\{x(t)\}$ es la transformada de Hilbert de $x(t)$.

La transformada de Hilbert H_x de la señal real $x(t)$ se puede expresar en dominio de Fourier como sigue:

$$TF[H_x](f) = (-j\ signe(f))X(f) \qquad \text{E8}$$

La extensión de la transformada de Hilbert al caso multidimensional no es trivial. La transformada de Fourier discreta, de la imagen analítica discreta es igual a cero en más de la mitad del plano de la frecuencia 2D.

Más de la mitad de la frecuencia del plano, es igual a dos veces la transformada discreta de Fourier de la imagen original de valores reales (excepto por 4 muestras de frecuencia que son idénticas a sus contrapartes en la transformada de Fourier discreta de la imagen original).

A. Bovik [12] da una práctica implementación de la extensión compleja $z(\mathrm{n1}, \mathrm{n2})$ de una imagen de $\mathrm{N} * \mathrm{M}$ de valores reales $\mathrm{f}(\mathrm{n1}, \mathrm{n2})$:

$$z(\mathrm{n1}, \mathrm{n2}) = \mathrm{f}(\mathrm{n1}, \mathrm{n2}) + j.\mathrm{g}(\mathrm{n1}, \mathrm{n2}) = f(n1, n2) + j.H[f(n1, n2] \qquad \text{E9}$$

En el dominio de Fourier esto se lee:

$$G(u,v) = TF[g(n1,n2)] = H(u,v).*F(u,v) \qquad \text{E10}$$

Donde

$H(u,v) =$ -j para u=1,2,…(N/2)-1
+j para u=(N/2)+1, (N/2)+2,…N-1
-j para u =0,v=1,2…(M/2)-1
-j para u =(N/2),v1,2,…(M/2)-1
+j para u =0,v=(M/2)+1, (M/2)+2,…M-1
+j para u =(N/2),v=(M/2)+1, (M/2)+2,…M-1

0 de otra manera.

Finalmente, $z(n1,n2)$ se obtiene tomando el inverso de la transformada de Fourier de $<< Z(u,v) = F(u,v) + j.G(u,v) >>$. Se puede usar un algoritmo más eficiente para calcular $Z(u,v)$ si se nota que para cada *u* y *v*, $Z(u,v)$ asume uno de solamente tres valores posibles: cero, $F(u,v)$ y $2F(u,v)$. La imagen de valores reales $f(\rho,\theta)$ se puede modelar como el siguiente modelo Q multi-componente:

$$f(\rho,\theta) = \sum_{q-1}^{Q} a_q(\rho,\theta).\cos[\varphi(\rho,\theta)] \qquad \text{E11}$$

Donde la función de (p, θ) es igual a la sumatoria desde q a la potencia -1, hasta Q de la multiplicación de $alpha_q$ (p, θ) por el coseno de [φ (p, θ)]

Primero, para aislar todos los componentes dominantes de *Q* contenidos en la textura, pasamos la imagen $f(\rho,\theta)$ a través de un banco-filtro paso-banda. Las respuestas del canal proporcionan una descomposición efectiva de componentes usando tres filtros paso-banda, que tienen un ancho de banda de un octavo. En el dominio de frecuencia, los filtros reales 2D no-defasores son diseñados por el producto de dos ventanas de Hamming $X_1(u)$ y $X_2(v)$:

$$X(u, v) = X_1(u).X_2(v) \qquad \text{E12}$$

Y

$$Xi(f) = \alpha_i + (1-\alpha_i)\cos\pi\frac{f - f_{qi}}{f_{oi}} \qquad \text{E13}$$

Donde fq_1 es la frecuencia central de cada filtro 1D X_1 a lo largo del eje de frecuencia (u o v). $f0_i$ Permite ajustar el ancho de banda de -3db a un octavo en función del fq_1 y a_1

$$f_{0i} = \frac{\Pi}{3.\arccos(\frac{1/2 - \alpha_i}{1-\alpha_i})} f_{qi} \qquad \text{E14}$$

Entonces los algoritmos de demodulación de un solo componente FM son aplicados directamente a las respuestas del canal para identificar las funciones de modulación del componente de FM usando la imagen analítica $z(\rho,\theta)$ como sigue:

$$\left|\Delta\varphi Di(\rho,\theta) = \arccos\left[\frac{z(\rho,\theta+1) + z(\rho,\theta-1)}{2z(\rho,\theta)}\right]\right| \qquad \text{E15}$$

Cualquier componente imaginario distinto a cero se debe desechar antes de la evaluación de la función del arcocoseno. En este caso la demodulación de frecuencia sólo se enfoca a la información horizontal importante a lo largo de θ en la representación rectangular de la textura del iris. Las tres frecuencias distintas dominantes de $\Delta\varphi Di(\rho,\theta)$ forman un vector de frecuencia emergente. Además podemos por supuesto también extraer la fase instantánea de $\varphi_i(\rho,\theta)$ introduciendo su expresión algebraica como sigue:

$$\rho i(\rho,\theta) = \arctan\frac{\mathrm{Im}(Z_i(\rho,\theta))}{\mathrm{Re}(Z_i(\rho,\theta))} \qquad \text{E16}$$

Dado que construir la imagen analítica implica una transformada de Hilbert 2D, que es una transformada global, la fase instantánea y la frecuencia emergente dependen de la señal entera. Las ventajas principales de usar la técnica analítica son: que es de cómputo eficiente: filtran en el dominio de Fou-

rier los filtros puros reales, y extrae la fase instantánea y/o la frecuencia emergente en cada posición (ρ,θ) en la textura del iris, y no necesitan mas cómputo (transformaciones globales).

3.4 Generación de código obtenido y análisis del iris

La codificación de las características del iris es similar al sistema de Daugman al mantener en el límite al módulo de la frecuencia emergente (E15), y a las partes real $\mathrm{Re}(\varphi_i(\rho,\theta))$ e imaginaria $Im\ (\varphi_i(\rho,\theta))$ de la fase instantánea $\varphi_i(\rho,\theta)$ (E16). Por lo tanto para una imagen rectangular de valores reales de tamaño N*M de la textura del iris, se dispone de nueve N*M imágenes binarias para hacer el código del iris. Sin embargo como el párpado o el punto la reflexión cubren algunas áreas del iris, el campo usable del código del iris se ajusta truncando pequeñas zonas de ruido en la zona como se muestra en la figura 3.4.

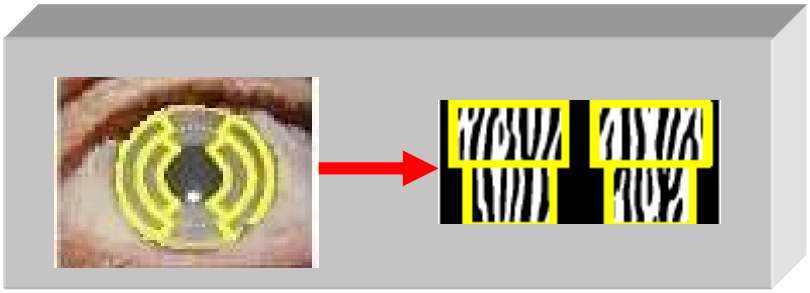

Figura (3.4 Código generado del iris)

El pasó final de la interpretación, realiza la prueba de distancia de Hamming, que se genera a partir del código del iris obtenido en tiempo real y de la plantilla del código del iris almacenada. De esta manera, la distancia *HD* de Hamming mide la fracción de bits que discrepan resultado de la comparación bit a bit de los dos códigos. En el caso del código de iris del impostor, o de un dato generado aleatoriamente, 0.5 es el valor previsto para HD. Un criterio, o umbral $(\in[0;0.5])$, se escoge y cualquier valor medido menor que este criterio es considera como identidad rechazada (falsa) mientras que los valores medidos mayores a este criterio se consideran como identidad verificada (auténtica). En la práctica, antes de la verificación bit a bit contra el código del iris en la base de datos, se recorre cada componente del código del iris (imagen binaria)

a lo largo de θ sobre un rango de orientaciones relativas (+/- 7° por ejemplo) a fin de considerar la posible inclinación de la cabeza durante la adquisición de la imagen del ojo.

3.5 Resultados experimentales

La figura 3.5.a, es una ilustración de la información representativa de la fase instantánea y de la frecuencia emergente, extraída a partir de dos imágenes del mismo iris, adquirido un tiempo diferente $(t_{0,}t_1)$. A pesar de la increíble similitud entre las imágenes, el sistema que se ha descrito proporciona una solución fiable para el procesamiento del iris.

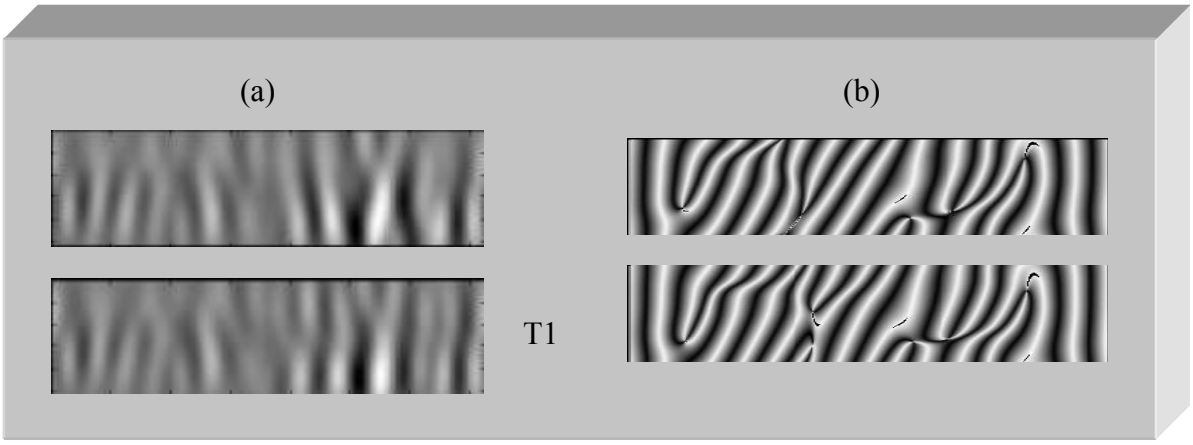

Figura (3.5.a Representación de la información del iris)
(a) Función instantánea de la fase.
(b) Función inesperada de la frecuencia.

En un estudio previo, se probo la combinación en una base de datos de 50 imágenes de iris adquiridas a partir de 5 personas que cooperaron (5 imágenes por ojo); el rango común del iris fue representado (lente de contacto, los cristales, etc.…). Al utilizar THGD[5] para localizar el centro del ojo en vez de aplicar solamente operadores integro diferenciales, permite evitar la mala detección del centro del iris cuando el punto espectral ocurre cerca de la frontera del iris (100% exitoso, contra el 86% sin el proceso previo).

[5] THGD: Gradient Decomposed Hough Transform, Transformada de Hough descomposición de gradiente

En un segundo estudio previamente experimentado, se estimaba la tasa de falsa aceptación y el índice de rechazo falso del sistema de reconocimiento del iris. Se preparó una base de datos de personal con más de 300 imágenes del iris (10 imágenes capturadas por ojo). Los códigos de iris de tamaño 768 bytes que se compararon en esa prueba incluyeron un muestreo de imágenes binarias producidas a través de las funciones de frecuencia emergente, en la figura 3.5.b se muestra la distribución observada en función de los dos tipos de población "personas auténticas" e "impostoras".

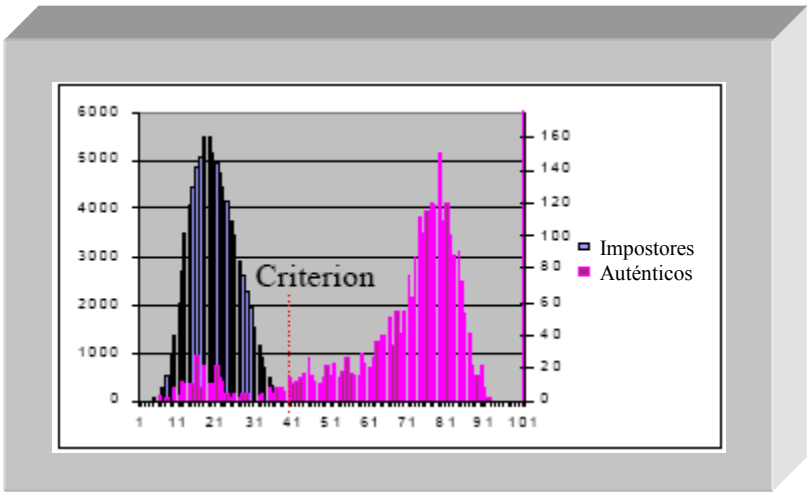

Figura (3.4.b Cuenta de distribución)

Por otra parte, una tercera base de datos de 40 imágenes del iris fue utilizada para enfrentar la "singularidad" de la frecuencia emergente con la singularidad de la fase local. Esta base de datos contuvo solamente imágenes manualmente pre-localizadas del iris a fin de cancelar la influencia de la localización inexacta en los procedimientos. En la figura 3.4.c se reportan las distribuciones de distancias de Hamming entre códigos de iris sin relación para los impostores y para los auténticos (códigos del iris del mismo tamaño). Podemos observar que la codificación de la frecuencia emergente parece ser tan pertinente como cifrar la fase local; en los dos casos la distribución está claramente separada, y no ocurre traslape.

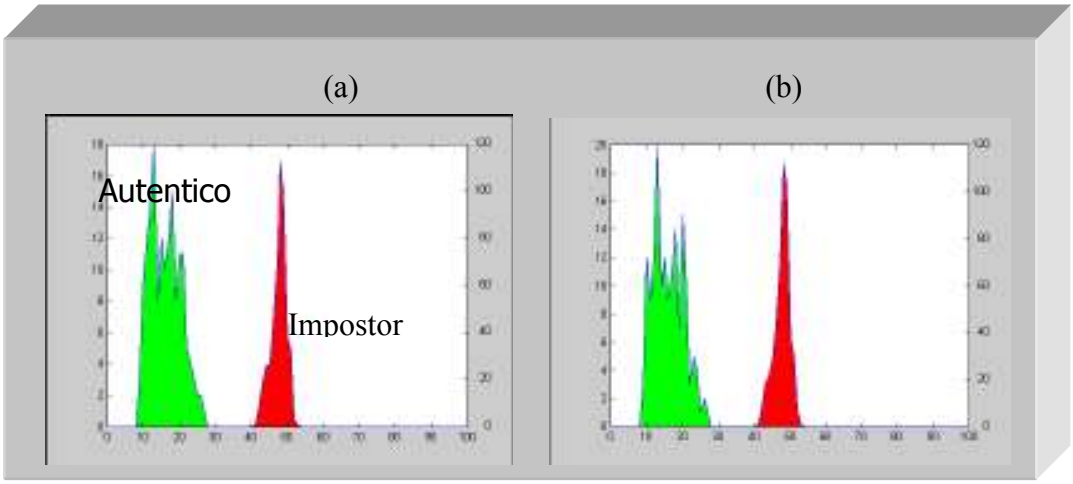

Figura 3.4.c Distancia de Hamming, distribución generada por:

(a) Los filtros de Gabor basados en un codificador de fase local.

(b) imagen analítica basada en un codificador de frecuencia emergente.

Conclusión

Implementar sistemas biométricos es lo más óptimo en cualquier sector público de la sociedad o privado ya que se tienen muchos beneficios; es cuestión de empezar desde las escuelas, instituciones y sectores bancarios, siempre y cuando no se viole la privacidad de las personas. La tecnología biométrica es el mejor método de identificación en sus diferentes ramas hoy en día, en comparación con los métodos tradicionales o comunes que hay, ya que las personas lejos de estar seguras con las claves habituales, están intranquilas al pensar que son inseguras.

La tecnología biométrica trae grandes beneficios a la sociedad ya que es más fácil evitar robos, extravíos, y falsificaciones de contraseñas habituales.

El cuerpo humano es único por lo tanto es una clave de acceso ilimitada en el uso de la biometría, ya que algunas partes del cuerpo humano no cambian nunca a lo largo de toda la vida.

La identificación del iris es la más recomendable para implementar, ya que tiene un alto grado de eficacia como se corroboró en el análisis de identificación con el método de Daugman.

Los sistemas biométricos de identificación funcionan mediante los datos que se almacenan en las bases de datos a través de un patrón biométrico de la persona y así el patrón biométrico podría estar entrelazado a un sistema de identificación de personas.

Posteriormente si esta persona tiene un accidente o comete una infracción y no quiere identificarse sería de muy buena utilidad solo captar alguna característica biométrica en un lector y saber de quien se trata, o si es quien dice ser, para evitar cualquier fraude o usurpación de claves.

Las personas interesadas en los sistemas de identificación biométrica solo tienen que adquirir un lector biométrico, un software para el reconocimiento biométrico, una técnica biométrica para la identificación del patrón biométrico, dándole un código de acceso a la persona a través de una computadora y así tener control de la seguridad de los bienes personales o información restringida de las personas.

Los sistemas de identificación son las llaves del futuro, es por eso que toda persona tiene que tomar en cuenta, que un sistema biométrico es uno de los métodos de identificación más seguros que hay y que mejor que estar a la vanguardia del mundo real; las personas debemos tomar en cuenta nuestra seguridad y que además de eso, con estos nuevos sistemas de identificación evitaríamos una replica de cualquier tipo de acceso a nuestro patrimonio o información de interés personal.

El implementar la tecnología biométrica a corto, mediano y largo plazo sólo nos trae una cosa, beneficios, tanto para rangos gubernamentales como empresariales en su información o bienes guardados, así como también estar al tanto del medio que colabora a nuestro alrededor o dándole un golpe a la impunidad que durante mucho tiempo ha podido burlar hasta la más alta seguridad mediante artimañas tan simples que hasta una persona promedio podría conseguir.

Las personas podemos decir que hoy ya no es ciencia ficción, como en años pasados lo veíamos en películas, y solo pensábamos que para que algo así nos tocara ver sería muy difícil, solo sabemos una cosa, no es ciencia ficción, si no el futuro en este presente, y en un presente que es muy exigente consigo mismo.

Como se explicó en al capitulo 2 los sistemas biométricos pueden clasificarse de acuerdo a sus característica y funcionalidad, por lo tanto su adquisición e implementación no debe verse como una actividad trivial o sin conse-

cuencias, en la realidad hay que saber cual escoger para poder cumplir con los requerimientos organizacionales y no causar incomodidades a las personas que lo van a utilizar por lo tanto expondremos a continuación los diferentes métodos biométricos existentes en el mercado y como funcionan, a fin de facilitar la elección de alguno según convenga a la persona o empresa que lo va adquirir.

Método	Exactitud	Costo	Usurpación	Facilidad de uso	Permanencia en el tiempo	Estabilidad	Aceptabilidad
Huella digital	Alta	Bajo	Si	Alta	No cambia	Alta	Muy alta
Forma de la mano	Alta	Medio	Si	Alta	Media (Solo el esqueleto)	Alta	Alta
Retina	Muy alta	Alto	No	Baja	Puede cambiar	Alta	Media
Iris	Muy alta	Alto	No	Media	No cambia	Alta	Media
Reconocimiento facial	Alta	Medio	No	Alta	Varia a menudo	Media	Media
Termografía	Alta	Medio	No	Alta	Varia a menudo	Media	Media
Olor	Muy alta	Medio	No	Alta	No cambia	Alta	Media
ADN	Muy alta	Medio	No	Alta	No cambia	Media	Media
Dinámica de trazado de la firma	Alta	Bajo	Si	Alta	Puede cambiar	Media	Muy alta
Forma de caminar	Alta	Medio	No	Alta	Puede cambiar	Media	Media
Voz	Alta	Bajo	No	Alta	Varia a menudo	Media	Alta
Golpeo o dinámica sobre el teclado de una computadora	Alta	Bajo	Si	Alta	Puede cambiar	Media	Media
Análisis Gestual	Alta	Bajo	No	Alta	Varia a menudo	Media	Media

Exactitud: La exactitud se refiere que tan preciso es el método biométrico, se determinó en 1) muy alta: ya que no presenta muchos errores, 2) alta: porque podría presentar algunos errores menores.

Costo: El costo hace referencia precio del sistema biométrico y todos los gastos relacionados, 1) bajo: significa que está al alcance del público en general, 2) medio: el costo podría ser ligeramente elevado, 3) alto: los costos son muy elevados.

Usurpación: La usurpación hace referencia a que si otra persona podría falsificar el patrón biométrico. 1) si: si se podría falsificar, 2) no: no es fácil de falsificar.

Facilidad de uso: La facilidad indica el nivel de complejidad del sistema y establece, por lo tanto, el nivel de experiencia o habilidad de la persona que está a cargo del sistema, 1) baja: no se requiere de ser un especialista, 2) Media: la persona a cargo podría ser un técnico, 3) alta: la persona a cargo del sistema tiene que tener los conocimientos necesarios en caso de un fallo del sistema y poderlos reparar.

Permanencia en el tiempo: La permanencia en el tiempo se refiere a la característica física de la persona conforme pasen los años. 1) no cambia: o cambia a lo largo de toda la vida, 2) media: podría cambiar el esqueleto, 3) puede cambiar: por alguna circunstancia externa podría cambiar, 4)varia a menudo: varia a menudo por que no siempre la persona esta en una misma condición.

Estabilidad: La estabilidad es una medida que establece que tan a menudo se tendría que estar monitoreando el funcionamiento tanto del sistema como de los lectores biométricos, 1) alta: constantemente se tiene que hacer limpieza en el lector biométrico, 2) media: Por lo general es cuando se llega a tener algún inconveniente con el sistema biométrico.

Aceptabilidad: La aceptabilidad que tiene el uso de la tecnología biométrica en la sociedad, 1) Muy alta: Las personas no tienen ningún inconveniente en el uso, b) Alta: Cuando las personas llegan a tener duda sobre el uso

pero lo aceptan, c) Media: las personas no se ven muy familiarizadas con su uso pero saben en que consiste.

Con ésta investigación ha sido posible identificar los beneficios y las utilidades de los sistemas biométricos en todos los sectores sociales. Utilizando la tecnología biométrica a las personas se les proporciona seguridad al saber que no pueden extraviar la llave biométrica por que ésta es el mismo cuerpo humano, dejando atrás las claves habituales. En los capítulos de esta investigación se expusieron cada uno de los conceptos relevantes de la biometría, así como el entendimiento de la tecnología biométrica en cada uno de sus conceptos y como funciona por medio del cuerpo humano junto con los diferentes métodos de identificación biométricos y los posibles errores que pudiesen arrojar como cuando son gemelos ó no se le da un buen uso al sistema o lector biométrico. La biometría constantemente va creciendo, lo cual le permitirá en un futuro ser un estándar de autentificación, en una gran cantidad de sectores.

Apéndice

ADN: "(ácido desoxirribonucleico) ácido nucleico compuesto de dos cadenas polinucleotídicas que se disponen alrededor de un eje central formando una doble hélice, capaz de autoreplicarse y codificar la síntesis de ARN. Lugar donde esta "depositada" la información genética. Ácido nucleico que funciona como soporte físico de la herencia en el 99% de las especies. La molécula, bicatenaria, ésta formada por dos cadenas antiparalelas y complementarias entre sí."[6]

NEC: National Electric Code es uno de los más grandes fabricantes de computadoras y electrónica del mundo.

FBI: "La Oficina Federal de Investigación es la agencia de espionaje con atribuciones para ejecutar acciones dentro del territorio estadounidense. En realidad, tiene categoría de Policía Federal puede actuar en cualquier estado de los Estados Unidos, pero una de sus misiones fundamentales es generar Inteligencia para la toma de decisiones en política interior. Es la más antigua de las agencias de Inteligencia. Fue fundada en 1908, aunque en1935 recibió el nombre con el que ahora es conocida"[7]

AFIS: "(Automated Fingerprint Identification) Tecnología para la identificación de huellas dactilares"

ULTRASONOGRAFIA: "Técnica radiológica de exploración del interior de un cuerpo mediante ondas electromagnéticas o acústicas, que registra las reflexiones o ecos que producen en su propagación las discontinuidades internas. Se emplea en medicina."[8]

---

[6] www.biologia.edu.ar/introduccion/4intro.htm

[7] http://www.venezuelafoia.info/glosario.html#FBI

[8] http://www.discapnet.es/Discapnet/Castellano/Glosario/E/Ecograf%C3%ADa+(ultrasonograf%C3%ADa).htm?pagina=1

CSL "Compressed Serial Line. "[9]

ANSI "American National Standards Institute o Instituto Americano de Normas Nacionales."[10]

NIST (National Institute of Standards and Technology) Instituto Nacional de Éstandares y Tecnología"

[9] http://www.tugurium.com/gti/termino.asp
[10] http://www.tugurium.com/gti/termino.asp

Bibliografía

[1] C. Tisse, L. Martin, L. Torres, and M. Robert. Person identification technique using human iris recognition. In *Proceedings. of Vision Interface*, paginas 294–299, (2002).

[2] Belt Ibérica
http://www.belt.es/expertos/experto.asp?id=2301

[3] Global Card 2000
http://www.globalcard2000.com/es/biometria/?bcsi_scan_D90DB3ADAF6F29C4=0

[4] Cippprs
http://www.cipprs.org/vi2002/pdf/s6-1.pdf

[5] Revista Detective
http://www.nec.cl/bases/i-510-2-1124301099.pdf

[6] A. K. Jain, A. Ross, and S. Pankanti.. A Prototype Hand Geometry-based Verification System. In *Proceedings of Second International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA)*, paginas 166-171, Washington D.C., USA. (1999d)

[7] A. Ross, K. Nandakumar and A. K. Jain. *Handbook of Multibiometrics,* Springer Science+Business Media, LLC ,pagina 51 (2006)

[8] El País
http://www.elpais.es/articulo/elpfutpor/20051123elpepifut_1/Tes/

[9] Bet Ibérica
http://www.belt.es/noticiasmdb/home2_noticias.asp?id=590

[10] Enciclopedia Wikipedia
http://es.wikipedia.org/wiki/Biometr%C3%ADa

[11] D y V Systems
http://mipagina.cantv.net/dyvsystems/news.htm

[12] A.C.Bovik,<< the handbook of image processing>>, Ed. Bovik.