UNIVERSIDAD NACIONAL AUTÓNOMA
DE MÉXICO

FACULTAD DE INGENIERÍA

PROPUESTA DE ESTÁNDAR PARA EL USO SEGURO DE TECNOLOGÍAS BIOMÉTRICAS

T E S I S P R O F E S I O N A L

QUE PARA OBTENER EL TÍTULO DE:

I N G E N I E R A E N C O M P U T A C I Ó N

P R E S E N T A

AVRIL HERNÁNDEZ BRIONES

DIRECTORA DE TESIS
M.C. MA. JAQUELINA LÓPEZ BARRIENTOS

MÉXICO, D. F., CIUDAD UNIVERSITARIA, 2009

A mi abuela Aurora Álvarez Lara (q.e.p.d)

No hay palabras que puedan expresar lo que significas para mí. El recuerdo de cada momento que compartimos juntas me llena de fuerzas para seguir luchando por todas aquellas cosas que anhelo. Siempre serás mi más grande ejemplo de amor incondicional y fortaleza.

A mi mamá

Gracias, Mil Gracias por tu infinito amor, no pude tener una mamá mejor que tú, sé que no ha sido fácil para ti así que gracias por no rendirte nunca y luchar por mí. Gracias también por todas las oportunidades que con tu esfuerzo me has brindado, sé que sin ti no estaría cumpliendo este sueño. Te amo con todo mi corazón.

A mi papá

Gracias por tu apoyo y amor incondicional, por estar siempre presente en los momentos más importantes de mi vida y por nunca dejar de creer en mí. Me siento muy orgullosa de tener un papá como tú. Te amo con todo mi corazón y este éxito también es tuyo.

A Dante

No importa lo lejos que estés, siempre te llevo conmigo y sé que voy contigo porque en lo que somos hoy, está presente lo que fuimos. A ti mi amigo del alma te doy las gracias por siempre porque hiciste que aquella época de caminar el mundo a corazón abierto fuera el mejor lugar donde esperar la vida. Te quiero.

A Zyanya

Gracias por tu infinito cariño y tu confianza, deseo que esto sirva como un incentivo para que te des cuenta que puedes lograr todas las metas que te propongas. Recuerda siempre que aquí nadie está loco, solo vive una realidad distinta (Jim Morrison).

A Rubén

Flakito, Gracias por llenar mi vida de magia, por darme la fuerza para seguir soñando, por hacerme tan feliz. Mil Gracias por dejarme entrar en tu corazón y por cada momento bonito e intenso que hemos compartido, deseo que sean muchos, muchos más.

"ej emia't"

A mis primos y mis tías

Gracias por su cariño y por estar cerca de mí y de mi familia. Gracias tía Rosy por tu ayuda, tus consejos y tus regaños, sin ti esto no sería posible.

A mis amigos Fátima Néquiz, Selene Armas, Atenea Armendáriz, Margarita Pineda, Daniel Aguilar, y Rodrigo Cabrera

Por cada uno de los momentos que hemos compartido, por su apoyo y amistad sincera. Los quiero, gracias por soportarme.

A la M.C. Ma. Jaquelina López Barrientos
Por su dedicación y apoyo incondicional en la elaboración de este trabajo. ¡¡Mil Gracias!!

ÍNDICE

INTRODUCCIÓN

En la actualidad, mantener segura la información que manejamos día a día, ya sea de manera personal, grupal o empresarial, se ha vuelto una necesidad básica, desafortunadamente la mayoría del mundo informático desconoce la magnitud del problema con el que se enfrenta y, generalmente, no se invierte ni el capital humano ni el económico necesarios para prevenir el daño o pérdida de información.

Lo que una persona tiene (clave de usuario) y lo que sabe (contraseña) ha sido por muchos años la base de la Seguridad Informática, sin embargo, la vulnerabilidad a la que están sujetas las organizaciones y los sistemas obliga a aumentar estas dos primeras garantías; el camino para ello es conformar un trinomio compuesto por los dos códigos referidos y por uno más, entendido como "lo que la persona es"; es decir, se trata de una clave basada en características únicas del ser humano, tanto fisiológicas como de comportamiento. A la tecnología que ofrece esta solución se le conoce como biometría.

Estas tecnologías de identificación de personas, basadas en mediciones de características biológicas y sociales se han vuelto un gran negocio para empresas de alta tecnología y un campo de estudio importante para científicos especializados en cómputo, matemáticas aplicadas, fisiología y ciencias del comportamiento.

Identificar con exactitud a las personas es muy importante y en cada caso, la complejidad de las técnicas empleadas dependerá del objetivo de la identificación: no es lo mismo determinar el sexo de una persona (para permitirle entrar a cierto lugar, un centro de convivencia por ejemplo), que identificar al legítimo propietario de una importante suma de dinero almacenada en un banco suizo.

Las tecnologías biométricas están evolucionando rápidamente y tienen un fuerte potencial que puede ser ampliamente usado en aplicaciones civiles que actualmente están presentando un rápido crecimiento como la banca electrónica, el comercio electrónico y el control de acceso. La seguridad informática es otro de los terrenos de aplicación, ya que varias laptops, teclados, ratones y memorias USB incluyen lectores de huella para que el usuario pueda proteger su información y llevar a cabo movimientos por Internet. Sin embargo, existen frenos naturales para el desarrollo de estas tecnologías y son las malas experiencias de los clientes, lo que se debe a la utilización de hardware o software biométrico que sólo colocaron por precio, pues hay factores más allá de éste que deben ser evaluados para aspectos tan importantes como lo son la seguridad y el control del personal; es justo aquí donde los estándares y la regulación también juegan un papel fundamental; no obstante ello, aún la estandarización se encuentra en proceso de desarrollo y como resultado de esta situación, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietarios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica 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). Existen además otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como: Biometrics Consortium, International Biometrics Groups y BioAPI.

Entre los estándares que se encuentran en uso actualmente a nivel internacional podemos encontrar el *Estándar ANSI X.9.84* que fue creado en el año 2001 por la ANSI (American National Standards Institute), el *Estándar ANSI / INCITS 358* creado en 2002 por ANSI y BioApi Consortium y finalmente el *Estándar NISTIR 6529* también conocido como CBEFF (Common Biometric Exchange File Format) que fue creado en 1999 por NIST y Biometrics Consortium.

En Argentina se cuenta con el *Estándar para la adquisición e Implementación de Sistemas Biométricos para Identificación y Verificación de Identidad* de *Institute of Electrical and Electronics Engineers* (IEEE), una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas, en cuyos capítulos se contemplan las condiciones a cumplir en lo pertinente al hardware, el software y las comunicaciones en implementaciones que contemplen brindar servicios de identificación de individuos por métodos biométricos utilizando herramientas informáticas.

Es por ello que se vuelve importante hacer conciencia sobre la importancia de contar con estándares; pues éstos no sólo permiten adquirir productos de alta calidad sino que se vuelven indispensables en la solución de las disputas entre comprador y vendedor, pues proporcionan un lenguaje mediante el cual se pueden comunicar sin ambigüedades, y de igual manera sirven como una "guía" a los productores para satisfacer de manera adecuada los requisitos de los consumidores facilitando de esa manera las relaciones comerciales. Sin embargo, un panorama completamente distinto se vive en nuestro país pues a la fecha no existe un organismo dedicado a la elaboración de estándares para este tipo de tecnologías. No obstante, la Norma Oficial Mexicana (NOM) y la Asociación Mexicana de Biometría e Identidad (AMBI) son dos organismos que ya contemplan su uso y regulación. Debido a esta falta de información es que se plantea como objetivo del presente trabajo realizar una propuesta de estándar de tecnologías biométricas para su uso seguro en el procesamiento de información en nuestro país.

Para ello el trabajo aquí desarrollado muestra en el **Capítulo I** los antecedentes históricos que dieron lugar al uso de la biometría como método de identificación y verificación de individuos y cómo se han desarrollado a lo largo de los años los diferentes sistemas de reconocimiento que hoy en día pueden ser aplicados en áreas como el Comercio electrónico o la Seguridad Informática.

Una vez establecido el panorama histórico y actual de la biometría, el **Capítulo II** nos proporciona las bases teóricas bajo las cuales se sustenta el desarrollo de los diversos sistemas biométricos, siendo la más importante el Reconocimiento de Patrones. Se muestran además las características de la arquitectura general de un sistema biométrico y

se hace una breve descripción de las medidas de desempeño que son usadas para evaluar el desempeño del sistema.

En el **Capítulo III** se hace una clasificación de los sistemas biométricos de acuerdo con el uso que se les da, con el tipo de aplicaciones que se desarrollan y con el tipo de características (físicas o conductuales) que éstos utilizan para llevar a cabo la verificación de la identidad de un individuo. Se proporciona también una descripción general del funcionamiento de las tecnologías biométricas con más presencia en el mercado.

En el **Capítulo IV** se establece la importancia de la elaboración y uso de estándares biométricos para el buen funcionamiento de las tecnologías desarrolladas y se enumeran las principales características de los estándares más conocidos como BAPI, BioAPI y X9.84 entre otros. Se menciona también el trabajo que en materia de estandarización realizan dos organismos mexicanos: la Asociación Mexicana de Biometría e Identidad (AMBI) cuyo principal objetivo es el de participar activamente en la generación de estándares y normas de identificación y la Dirección General de Normas (DGN) que se encarga de elaborar las normas oficiales mexicanas.

Hasta el momento estos organismos no han participado en el desarrollo de normas o estándares que regulen el uso de este tipo de tecnologías en el país, por ello en el **Capítulo V** se desarrolla una propuesta de estándar cuyo objetivo es servir como una guía para asegurar el uso óptimo y seguro de las tecnologías biométricas utilizadas en el procesamiento de información. Para elaborar esta propuesta se tomaron en cuenta aspectos como la seguridad física de los dispositivos, la seguridad ligada a los usuarios y las vulnerabilidades a las que están expuestos los sistemas biométricos.

Finalmente el **Capítulo VI** muestra las características generales de las diferentes alternativas tecnológicas que se tomaron en cuenta para la difusión de la información recopilada en este trabajo. De igual forma se proporciona una muestra del diseño de la tecnología utilizada y las secciones que la conforman.

CAPÍTULO I

Fundamentos de Biometría

I.1. Antecedentes Históricos.

La Identidad, lo que permite distinguir a un individuo de los demás, resulta de una combinación de rasgos biológicos (físicos) y sociales (conductuales) que le son intrínsecos: la forma de la cara, la estatura, el color de ojos, la conformación de la dentadura, son ejemplos típicos de elementos constituyentes de la identidad biológica de una persona. Los rasgos sociales son en gran parte resultado de la interacción del individuo con su medio y en cierta manera almacenan información sobre la naturaleza de dicha interacción.

La práctica tecnológica de identificar a un individuo por sus rasgos biológicos y conductuales recibe el nombre de *Biometría*; cuando tiene lugar de manera automatizada, mediante técnicas matemáticas auxiliadas por computadora, se conoce como *Biometría informática* (véase figura 1.1). La identidad así construida se denomina identidad biométrica del individuo.

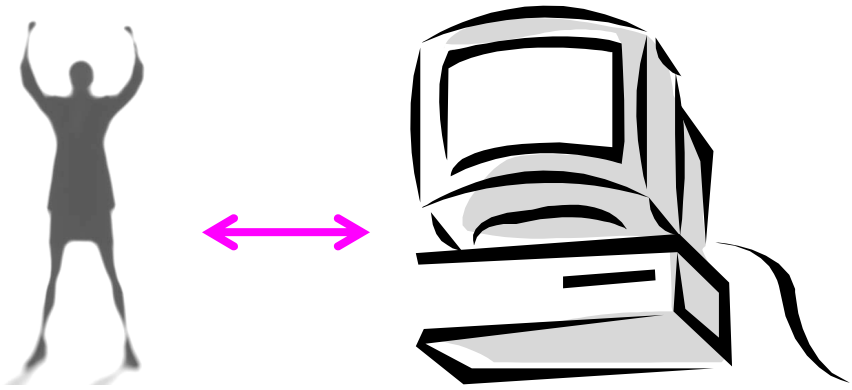


Figura 1.1 Biometría informática.

Si entendemos este concepto podemos darnos cuenta que el ejercicio de identificación de personas lo llevamos a cabo diariamente y casi sin darnos cuenta; por ejemplo, cuando hablamos por teléfono y oímos la voz de nuestro interlocutor nuestro cerebro trata de comprobar si esa voz se parece a cualquiera de las muestras que tiene almacenadas y que ha ido recopilando a lo largo de nuestra vida, si es que el cerebro encuentra similitudes suficientes entre alguna de las muestras y lo que está escuchando entonces puede identificar al interlocutor. Cabe mencionar que esta práctica ya se llevaba a cabo en tiempos antiguos donde haciendo uso de las características físicas de los individuos, los egipcios verificaban la identidad de las personas que participaban en las diferentes operaciones comerciales y judiciales. Lo mismo ocurría en las zonas agrícolas de diversos países donde las cosechas eran almacenadas 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 éstos hicieran algún retiro de su mercancía.

Se sabe que en el siglo XIV en China, los mercaderes estampaban las huellas de la palma de la mano y los pies de los niños en un papel con tinta para distinguir a los niños uno de otro.

En el siglo XIX investigadores en criminología intentaron relacionar las características físicas de los individuos con tendencias criminales, por ejemplo, Alphonse Bertillon desarrolló el sistema "Bertillonaje" o antropometría descriptiva como un método para identificar individuos basado en registros detallados de medidas de su cuerpo. No obstante los resultados no eran concluyentes, pero la idea de medir las características físicas de un individuo parecía efectiva. De manera paralela comenzó el desarrollo de la identificación de huellas dactilares que muy pronto se convirtió en la metodología internacional para la identificación debido a que éstas son un rasgo distintivo entre los seres humanos. En 1856, sir William Herschel fue el primero en implantar la huella dactilar como método de identificación en documentos para personas analfabetas. El 28 de Octubre de 1880 Henry Faulds, un médico escocés que trabajaba en Tokyo, publicó un artículo en la revista Nature sobre cómo identificar criminales a partir de sus huellas dactilares llamado “On the Skin-Furrows of the Hand”.

En 1892 Sir Francis Galton, primo del célebre Charles Darwin, publicó el libro "Finger Prints" (véase figura 1.2), que contenía un estudio detallado de las huellas dactilares y en donde además presentó un nuevo método de clasificación usando las huellas dactilares de los 10 dedos de las manos. En este método de clasificación (en uso hoy en día) identifica las características por las que las huellas dactilares pueden ser clasificadas. Su hijo, quien continuó su investigación, estableció el cálculo de probabilidad de que dos huellas sean iguales en 1:64.000.000.000. Este sistema fue llamado Galtoneano o Icnofalangometría. Galton también enunció las tres leyes fundamentales de la Dactiloscopia: perennidad, inmutabilidad y diversidad infinita, cada una de las cuales se verá a detalle en el Capítulo III.

Figura 1.2 Portada del libro “Finger Prints” escrito por Sir Francis Galton.

Las características propuestas por Galton para la clasificación de las impresiones dactilares fueron analizadas y mejoradas por el investigador de la Policía de la provincia de Buenos Aires Juan Vucetich a quien el Jefe de Policía ,Guillermo J. Núñez, le había encomendado sentar las bases de una identificación personal confiable. Vucetich usó inicialmente 101 rasgos de las huellas para clasificarlas en cuatro grandes grupos. Posteriormente logró simplificar el método basándolo en cuatro rasgos principales, los cuales se verán a detalle en el capítulo III: arcos, presillas internas, presillas externas y verticilos. Con base en sus métodos, la policía bonaerense inició en 1891, por primera vez en el mundo, el registro dactiloscópico de las personas. En el año 1892 se llevó a cabo por primera vez la identificación de una asesina, con base en las huellas dejadas por sus dedos ensangrentados (en particular por su pulgar derecho)

en la escena del crimen de sus dos hijos, en la ciudad de Necochea (provincia de Buenos Aires). Esta mujer, de nombre Francisca Rojas, había acusado de los asesinatos a un vecino. Luego de más de un siglo de su implantación la identificación de personas a través de huellas dactilares todavía se basa en los cuatro rasgos propuestos por Vucetich.

Entre 1905 y 1908 se implementa el uso de sistemas de huellas dactilares en la Fuerza Aérea, Ejército y Armada de Estados Unidos.

A partir del año 1935 se comenzaron a utilizar otras características físicas como variantes de identificación, por ejemplo el iris del ojo, en este sentido, los oftalmólogos Carleton Simon e Isodore Goldstein escribieron un artículo para el New York State Journal of Medicine que fue publicado en Septiembre de ese mismo año y se tituló "A new Scientific Method of Identification", en este artículo plantearon que los patrones vasculares de la retina son únicos en cada individuo. El siguiente año el oftalmólogo Frank Burch propuso el concepto de usar los patrones del iris como método de reconocimiento individual.

En el año de 1941, Murray Hill de los Laboratorios Bell inició el estudio de la identificación por voz, sus trabajos fueron redefinidos por L.G. Kersta.

Durante los años 1964 y 1965 Woodrow Wilson Bledsoe, Helen Chan Wolf y Charles Bisson trabajaron en el reconocimiento facial humano haciendo uso de la computadora y desarrollaron el primer sistema semi-automático de reconocimiento.

La Aviación Norteamericana desarrolló el primer sistema de reconocimiento de firma manuscrita en 1965.

En 1969 el Buró Federal de Investigaciones (FBI) impulsó a automatizar el proceso de reconocimiento de huella dactilar pues éste requería de muchas horas hombre para el proceso manual, para lo cual contactando al Buró Nacional de Estándares (NBS), ahora Instituto Nacional de Estándares y Tecnología (NIST) para que estudiaran el proceso de automatización de identificación de huellas dactilares.

Ese mismo año, el 25 de Noviembre, Salvatore R. Danna patentó en Estados Unidos un instrumento para identificar la firma con la patente No. 3480911 (véase figura 1.3), asignada a Conetta Manufacturing Company.

United States Patent Office 3,480,911 Patented Nov. 25, 1969

1

3,480,911
SIGNATURE IDENTIFICATION INSTRUMENT
Salvatore R. Danna, Ridgefield, Conn., assignor to Conetta Manufacturing Company, Inc., Stamford, Conn.
Filed Oct. 20, 1965, Ser. No. 498,604
Int. Cl. G01l 3/24, 1/18; G01d 1/00
U.S. Cl. 340—146.3 9 Claims

ABSTRACT OF THE DISCLOSURE

A signature identification instrument in which the pressure exerted by a person's handwriting produces signals which are a function of the number of times predetermined writing pressure is applied and the duration of the application of each writing pressure.

This invention relates to identification systems and more particularly to systems for identifying writings, such as handwritten signatures.

Banks, stores, and similar organizations, which deal in commercial paper such as checks, require means for immediately determining that an individual signing his name in the presence of one of their employees is actually the person having an account. Further, many industrial and military facilities require that an individual be cleared for security purposes before being permitted to enter the premises. Today, in cashing checks of individuals, banks still rely primarily on a visual inspection of an individual's signature. For organizations which require security clearances, they rely primarily upon the use of an identification badge with a photo insert, which is shown to a guard prior to entering the premises. In both of these cases, forgery and misrepresentation are still possible.

Accordingly, a new and improved system for identifying an individual's signature was required. Not only must this system be capable of supplanting or complementing visual inspections, but it must also be capable of functioning such that an identification of the individual is completed soon after the individual has written his signature.

In view of the foregoing considerations, the present invention provides for means for determining that an individual signing his name is actually the person he purports to be.

Furthermore, this system provides a means for easily detecting a forger, as well as someone misrepresenting himself as another.

Accordingly, an object of this invention is to provide a new and improved writing identification system.

Another object of this invention is to provide a new and improved writing identification device wherein the output signal from the device is related to certain characteristics of the individual to be identified.

A further object of this invention is to provide a new and improved signature identification device wherein the output signal is related to both the number of times an individual contacts a surface in writing his signature as well as the amount of time it actually takes one to write his signature every time he contacts the surface.

Still other objects and advantages of the invention will in part be obvious and will in part appear hereinafter.

In accordance with this invention, an identification device is provided which includes means for detecting that a force greater than a predetermined force is being applied by an individual during the time he writes his signature and second means responsive to said first means for providing an output signal indicative of both time and break characteristics of an individual while writing his signature. In a preferred embodiment of this invention, the handwritten signature is identified by providing a surface means for writing thereon, a first means responsive to writing on the surface for providing a first signal indicating that a force greater than a predetermined amount of force is being applied to said surface during the writing, and the second means responsive to said first means providing an output signal related to both the number of times the person writes on the surface with a sufficient force and the time intervals the sufficient force is applied while the person writes.

The invention accordingly comprises the apparatus possessing the features, properties and relation of elements which will be exemplified in the apparatus hereinafter described and the scope of the invention will be indicated in the claims.

For a fuller understanding of the nature and objects of the invention, reference should be had to the following detailed description, taken in conjunction with the accompanying drawings, in which the same reference numerals designate like or corresponding parts in the several views and, in which

FIG. 1 is a block diagram of the identification device according to the preferred embodiment of this invention;

FIG. 2 is a schematic wiring diagram partially in block form, of an electrical circuit suitable for use as the device shown in FIG. 1;

FIG. 3 is a perspective view of the device embodying this invention;

FIG. 4 is a top plan view with the cover of the device removed, showing the working parts and the writing surface according to this invention;

FIG. 5 is a side elevational view of FIG. 4, with certain parts omitted;

FIG. 6 is a diagram of the card which may be substituted for a paper roll, according to this invention; and

FIG. 7 is a block diagram of an alternate embodiment of this invention.

Referring now to FIGS. 1–5, there is disclosed a pressure sensitive transducer **10** which provides an output signal indicating that a force or pressure of a certain amount has been applied. In accordance with the preferred embodiment of this invention, the force is detected by utilizing a surface **11** (see FIGS. 4 and 5) over which there flows paper **12** from a plurality of rolls **13** and **14** driven by a motor **15**. The plate **11** is connected to side members **16a** and **16b** which are pivotally supported from members **17** and **18** and is balanced by the use of plates **19** and **20**. Extending from the plate or writing surface **11** is a member **21** which abuts contacts **23** and **24** mounted in a supporting block **25**. The transducer, including the surface **11**, is positioned within a device casing **30** as shown in FIG. 3, so that an individual may write his name in a cut-out portion **31**. The individual writes his name with any usual type of writing implement, such as a ball point pen, in the space provided in the top cover of the device. Upon initiation of the writing of the individual's signature, plate **11** will be depressed to close contacts **23** and **24** when a sufficient force is applied. Although in the preferred embodiment the use of contacts are shown because of their simplicity, it is to be understood that strain transducers, strain gages, strain-sensitive diodes and transistors and more sophisticated semi-conductor devices may be utilized in place of the contacts **23** and **24**, as long as a signal is provided which indicates that an individual is supplying sufficient force during the writing of his name on the surface **11**. The transducer **10** is coupled to a pair of selectors, shown at **40** and **41**, which are in turn coupled to a plurality of pulse counters **44–47** in a predetermined manner, as shown in FIG. 1. The manner in which the counters are

Figura 1.3 Hoja principal de la patente de Salvatore R. Danna.

En los setentas A.J. Goldstein, L.D. Harmon, y A.B. Lesk usaron 22 marcas específicas subjetivas como el color de cabello y grosor de labios para automatizar el reconocimiento facial. El problema con estas soluciones es que las mediciones y localización eran digitadas manualmente. En Mayo de 1971 publicaron en Proceedings of the IEEE un artículo sobre el tema, titulado "Identification of human faces".

El 25 de Mayo de 1971 se patenta en Estados Unidos un sistema de identificación de la palma de la mano por parte de Norman G. Altman.

En 1975, El FBI fundó el desarrollo de escáneres de huella dactilar para clasificadores automatizados y tecnología de extracción de minucias, lo cual condujo al desarrollo de un lector prototipo. Este primer lector usaba técnicas capacitivas para recoger las minucias. En ese momento sólo los datos biográficos de los individuos, la clasificación de los datos de huellas dactilares y las minucias eran almacenados a causa de que el costo de almacenamiento de las imágenes digitales de las huellas dactilares era prohibitivo.

La tecnología de huellas dactilares continuó mejorando y para el año 1981, cinco sistemas automatizados de identificación por huella dactilar fueron desplegados. Varios sistemas estatales en los Estados Unidos y otros países habían implementado sus propios sistemas autónomos, desarrollados por un número de diferentes proveedores. Durante esta evolución, la comunicación y el intercambio de información entre sistemas fueron pasados por alto, significando que una huella dactilar recogida con un sistema no podía ser buscado en otro sistema. Estos descuidos llevaron a la necesidad y al desarrollo de estándares para huellas dactilares.

Durante la última década la industria de la biometría ha madurado y la investigación de las tecnologías biométricas orientada al mercado empresarial y de la seguridad comienza a tener un crecimiento significativo. En la actualidad comienzan a aparecer en el mercado aplicaciones a gran escala que serán cada vez más accesibles para empresas y particulares.

En México, por ejemplo, la biometría apenas empieza como práctica tecnológica vinculada a la seguridad informática. En 2004 a 18 agentes de la Procuraduría General de la República, incluyendo al entonces Procurador General de la República, Rafael Macedo de la Concha, se les implantó bajo la piel una versión especial del sistema RFID (Identificación Por Radiofrecuencia, por sus siglas en inglés) que consiste en un chip que contiene información y que puede ser leído a distancia. Según el artículo "El Reinado de la Biometría" publicado en la revista ¿Cómo ves? de Julio de 2007, Año 9, No.104, el dispositivo fue implantado de manera voluntaria. El dispositivo electrónico de un tamaño menor al de un grano de arroz (véase figura 1.4), permite identificar cuándo un agente etiquetado entra en contacto con documentos confidenciales y puede también guardar información personal como su nombre, dirección, teléfono, y hasta una fotografía. Si bien esta aplicación tecnológica parece legítima, es importante reflexionar hasta qué punto se está afectando el derecho a la privacidad y nuestra salud pues pese a haber sido aprobados para uso humano por la estadounidense Food and Drugs Administration, equivalente a la Secretaría de Salud, no son inocuos. Contienen vidrio y metal, así que si lleva uno de ellos, deberá olvidarse de someterse a estudios de rayos X o a radiaciones como resonancias magnéticas, porque se le puede calcinar el chip dentro del brazo y quemarle. También existe el riesgo de que el implante, una vez dentro del brazo, se mueva y se coloque en un lugar peligroso. Sobre el supuesto de que la cubierta de cristal se rompa estando dentro del brazo, algo que sucedería gracias a un inoportuno golpe, no se ha dicho nada tampoco. Se ha descubierto también que los chips resultan altamente cancerígenos. Además, la tecnología RFID todavía no está lista para utilizarse en aplicaciones tan delicadas como la identificación de personas o el control de acceso a zonas restringidas esto debido a que varios científicos han podido realizar "clones" del chip.

Como con toda aplicación tecnológica, es el respeto a la dignidad humana lo que debe guiar la evolución de la biometría, para evitar que su uso se convierta en una pesadilla.

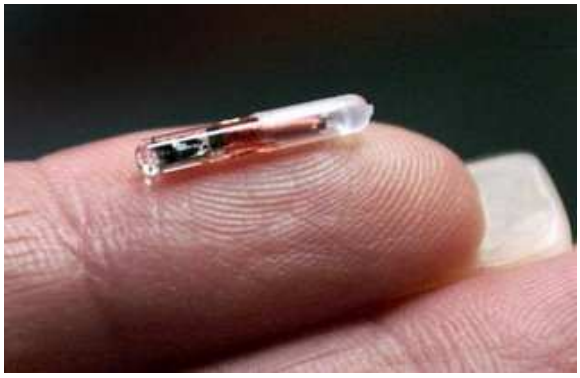


Figura 1.4 Dispositivo RDIF.

I.2. Necesidad y Objetivo de la Biometría.

Actualmente, los sistemas de identificación tradicionales no dan abasto para la creciente demanda de seguridad de las empresas pues éstas requieren verificar con precisión la identidad del personal que puede acceder a sitios restringidos o bien a cierta información de carácter confidencial. De ahí la necesidad de implementar sistemas que empleen la biometría y sus ventajas como método de identificación pues mediante su uso no existe la posibilidad de compartir claves, códigos de ingreso ni tarjetas de acceso, además de que se considera que la posibilidad de suplantar la identidad del individuo es prácticamente imposible. Lamentablemente éste es un reto que la ciencia y la tecnología aún no han superado pues aunque algunos de estos sistemas son altamente fiables, ninguno es cien por ciento efectivo pues son susceptibles de ser engañados mediante suplantación, por ejemplo, sistemas de reconocimiento de huella dactilar pueden ser fácilmente engañados usando un molde del dedo realizado con gelatina o simplemente disponer de la huella dactilar.

Encontrar un sistema infalible e inequívoco para reconocer personas es el objetivo de la biometría.

I.3. Aplicaciones.

Como ya hemos visto, la biometría ha sido ampliamente usada en aplicaciones como identificación de criminales y la seguridad en prisiones. Este tipo de tecnología está evolucionando rápidamente y tiene un fuerte potencial que hace que sea especialmente interesante en determinadas áreas, de entre las cuales la Seguridad Informática es una de las más recientes.

I.3.1. Banca Electrónica y Comercio Electrónico.

Ésta ha sido una de las áreas que mayor crecimiento ha tenido en los últimos años y la que más ha influido en el desarrollo de nuevos sistemas de seguridad, hasta el punto de que la idea en este sector es reducir los precios de venta de los dispositivos de reconocimiento biométrico hasta que acaben formando parte de la computadora, integrados incluso en el mouse o teclado por ejemplo, detectores de huella dactilar, sensores de presión y velocidad de tecleo o webcams con reconocimiento facial.
La principal ventaja que ofrecen tanto la banca como el comercio electrónico es la posibilidad de acceder a los servicios electrónicos a través de cualquier computadora que cuente con acceso a internet. Sin embargo, existe la posibilidad de que el sistema en uso no sea cien por ciento seguro pues todo lo que el ser humano crea puede ser mejorado o vulnerado por otro ser humano. De esta forma el uso de tecnología biométrica ofrece la seguridad tanto a la empresa como al individuo de que la operación que se realice a través de internet es llevada a cabo de manera confiable.

I.3.2. Aeropuertos.

A partir de los atentados del 11 de Septiembre de 2001 en Estados Unidos la necesidad de seguridad aeroportuaria tuvo un incremento substancial. Además de hacer uso de la seguridad física se comenzó a utilizar la tecnología biométrica en programas de iniciativa privada apoyados por el gobierno como el denominado Viajero Registrado (Registered Traveler) y el programa Iniciativa de Fronteras Seguras (SBI) del Departamento de Seguridad Interna de Estados Unidos.

El uso de este tipo de tecnología atrajo profundamente el interés entre los expertos en seguridad aérea, por lo que una gran variedad de aplicaciones comenzó a circular por los aeropuertos en todo el mundo. En Estados Unidos, el aeropuerto de Chicago, el segundo más grande del mundo, fue uno de los pioneros en emplear estos sistemas, al probar entre sus trabajadores un método de identificación a través de huellas dactilares de la empresa SecuGen, iniciativa que luego siguieron otros aeropuertos estadounidenses como el de San Francisco, Houston y Oakland.

Mientras los sistemas biométricos de identificación se implementaban de forma casi generalizada en las instalaciones aeroportuarias de EEUU, en Europa la adopción fue mucho más lenta, de manera que sólo en grandes aeropuertos como el de Schipol en Amsterdam, y el Heathrow en Londres, habían empezado a utilizar estos sistemas de reconocimiento.

Entre las medidas de seguridad aeroportuaria que se han implementado recientemente se encuentra el uso del *pasaporte biométrico* que puede ser leído mecánicamente y está provisto con un chip electrónico que contiene toda la información biométrica de la persona. El 6 de Septiembre de 2006 se emitió el primer pasaporte biométrico cuyo destinatario fue Atzo Nicolaï, Ministro de Renovación Gubernamental y Relaciones del Reino en Holanda. En Estados Unidos ya existe una ley que requiere que todo visitante internacional tenga visa o cualquier otro documento que use identificación biométrica, así lo establece esta disposición a las embajadas y consulados de los Estados Unidos, y que, por el constante trasiego de visitantes y emigrantes de diferentes parte del mundo a la nación estadounidense, los demás países se han visto en la obligación de aplicar.

1.3.3. Seguridad Informática.

La cada vez mayor dependencia tecnológica de las organizaciones e individuos para la realización de sus actividades, traducida en el uso generalizado de Internet y sus servicios, sistemas de información, computadoras portátiles, de escritorio, las agendas electrónicas y las tecnologías inalámbricas, han hecho que el acceso a datos e información sea más fácil que antes. Lo que desde otra perspectiva ha generado nuevas oportunidades para el surgimiento de problemas relacionados con la tecnología tales como el robo de datos, los ataques maliciosos mediante virus, el crackeo a los equipos de cómputo y redes de computadoras, entre otros, por lo que podemos clasificar en tres grandes grupos las aplicaciones que son más susceptibles a sufrir ataques como consecuencia de esta evolución:

1. A sitios (Centros de Cómputo)

La seguridad física debe ser empleada junto con la seguridad administrativa y técnica para brindar una protección completa a los equipos de cómputo. Ninguna cantidad de seguridad física puede proteger la información confidencial si no se controla el acceso físico a los servidores y equipos. Este tipo de acceso es muy importante pues todos los equipos delicados deben estar protegidos del acceso no autorizado; normalmente esto se consigue aglomerando los sistemas en un centro de datos. Este centro puede estar controlado de diferentes maneras entre las cuales, las tecnologías biométricas, ofrecen una gama amplia de opciones como puede ser por ejemplo un lector de huella dactilar, un lector de iris o retina, un sistema reconocedor de voz, un sistema de reconocimiento facial, entre otros.

2. A redes

Hoy en día la mayoría de las personas dependemos de la información que radica y generamos en nuestras computadoras y éstas ya no se encuentran aisladas como en los años 80 y principios de los años 90; sino por el contrario, hoy dependemos de una conexión física para podernos comunicar, el avance que se ha tenido con las redes nos ha permitido solucionar problemas y hacer provecho de sistemas que nos ayudan a manipular la información. Empresas, organizaciones y cualquier persona que utiliza una computadora envía y recibe correos electrónicos, comparte información de manera local o a nivel mundial, realiza transacciones, ofrece servicios y encuentra soluciones a sus requerimientos. Es así que la información se vuelve algo muy preciado tanto para los usuarios como para los Hackers. Es por eso que se hace necesario tomar una serie de precauciones para evitar que alguien no deseado busque en nuestra información y seamos presa fácil de extorsiones, fraudes y pérdidas irreparables, para ello existen sistemas de acceso a redes y computadoras que remplazan el uso de las contraseñas convencionales por el uso de biometría de impresión dactilar. Un ejemplo de este tipo de solución son los sistemas FS80 FinLogon, los cuales integran el reconocimiento de huellas dactilares al sistema de control de acceso de plataformas Windows. Este sistema está disponible en dos versiones:

* FinLogon PE (Personal Edition). Es la versión para las computadoras personales o de escritorio que trabajan con los sistemas operativos Windows 2000 y/o Windows XP. La información biométrica se almacena en el registro de Windows en forma encriptada (AES de 256 bits).

* FinLogon EE (Enterprise Edition). Es la versión para redes en Active Directory. Los componentes centrales del FinLogon EE se instalan en servidores Windows 2000/2003, mientras que las computadoras cliente soportadas son aquellas que trabajan con Windows 2000 y/o Windows XP. La información biométrica se almacena en Active Directory en forma encriptada (AES de 256 bits).

3. A equipos personales

Para proteger la información que resguardamos ya sea en nuestras Computadoras portátiles o de escritorio es necesario implementar soluciones de identificación de

usuarios, para que la información que requiera protección sólo sea accedida por personas autorizadas, lo cual puede ser llevado a cabo usando tecnologías biométricas. Actualmente existen diversos dispositivos en el mercado como memorias USB, teclados y mouses con tecnología biométrica de huellas dactilares cuya función principal es el proteger la computadora de la entrada de personas no autorizadas. Así mismo se encuentra en el mercado la computadora portátil Ideapad de la marca Lenovo (véase figura 1.5) que incorpora una función de inicio de sesiones mediante reconocimiento biométrico del rostro del propietario; la computadora capta una imagen del propietario y la compara con una base de datos de sus usuarios.

Figura 1.5 Computadora portátil Ideapad marca Lenovo.

1.3.4. Control de Acceso.

Hasta hace no mucho tiempo los dispositivos de control de acceso podían ser desde una puerta blindada hasta una reja o portal, pasando por torniquetes o cualquier medio de gestión de acceso, sin embargo, la apertura de una puerta o el acceso a áreas restringidas de una entidad ya son también un tema resuelto por la biometría. El uso de este tipo de tecnologías se ha convertido en la solución para muchas empresas pues como ya se ha mencionado, la finalidad de éstas radica en permitir que sólo el personal autorizado ingrese a un ámbito o lugar específico además de evitar el tráfico de contraseñas y tarjetas de identificación.

Conjuntamente el uso de tecnologías biométricas asegura que cada uno de los empleados de la empresa esté plenamente identificado y sea insustituible haciendo prácticamente imposible que un empleado registre la asistencia de otro.

CAPÍTULO II

Bases Teóricas y Sistemas Biométricos

II.1. Reconocimiento de Patrones.

El reconocimiento de patrones es la ciencia que se encarga de la descripción y clasificación (reconocimiento) de objetos, personas, señales, representaciones, etc. Esta ciencia trabaja con base en un conjunto previamente establecido de todos los posibles objetos (patrones) individuales a reconocer. El margen de aplicaciones del reconocimiento de patrones es muy amplio, sin embargo, las más importantes están relacionadas con la visión y audición por parte de una máquina, de forma análoga a los seres humanos.
El esquema de un sistema de reconocimiento de patrones consta de varias etapas relacionadas entre sí (los resultados de una etapa pueden modificar los parámetros de etapas anteriores). La figura 2.1 muestra un esquema general de un sistema de reconocimiento de patrones, en el cual el sensor tiene como propósito proporcionar una representación factible de los elementos del universo a ser clasificados. Es un sub-sistema crucial ya que determina los límites en el rendimiento de todo el sistema. La Extracción de Características es la etapa que se encarga, a partir del patrón de representación, de extraer la información discriminatoria eliminando la información redundante e irrelevante.
El Clasificador es la etapa de toma de decisiones en el sistema. Su rol es asignar los patrones de clase desconocida a la categoría apropiada.

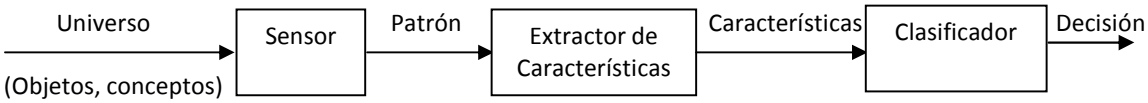


Figura 2.1 Esquema general de un sistema de reconocimiento de patrones.

El objetivo de estas etapas es ajustar el sistema para que sea capaz de clasificar señales u objetos de entrada en una de las clases predefinidas. Para ello deberá analizar un cierto número de características y para poder clasificar satisfactoriamente señales de entrada, es necesario un proceso de aprendizaje en el cual el sistema crea un modelo de cada una de las clases a partir de una secuencia de entrenamiento o conjunto de vectores de características de cada una de las clases. Generalmente se acepta que la secuencia de muestras de entrenamiento debe contener para cada una de las clases un mínimo de elementos igual a diez veces la dimensión de los vectores de características.
El sistema de reconocimiento de patrones debe tener en cuenta las fuentes de variabilidad como son el ruido, rotaciones, cambio de escala y deformaciones, lo cual se logra incluyendo en la secuencia de entrenamiento patrones que hayan experimentado estas modificaciones.

Como se puede observar, el reconocimiento de patrones es la base teórica más importante de la biometría pues un sistema biométrico es, en esencia, un sistema de reconocimiento de patrones, razón por la cual el estudio de las bases matemáticas sobre las cuales se sustenta esta ciencia se vuelve de vital importancia para los fabricantes de tecnología biométrica, no así para el desarrollo de este trabajo de tesis cuyo objetivo es

realizar una propuesta de estándar para el uso seguro de las tecnologías biométricas en el procesamiento de información.

II.2. Fisiología.

La fisiología estudia las funciones de los seres vivos y el cómo un organismo lleva a cabo las diversas actividades vitales: cómo siente, cómo se mueve, cómo se adapta a unas circunstancias cambiantes, y cómo da lugar a nuevas generaciones.
El término fisiología fue utilizado por Aristóteles (384-322 a.C.) para describir el funcionamiento de todos los organismos vivientes y por Hipócrates (460-377 a.C.) que lo asociaba al "poder curativo de la naturaleza". A lo largo del siglo XVI en Europa el término se asoció definitivamente con el estudio de las funciones vitales del cuerpo humano, extendiéndose más adelante al de los animales y plantas. En contraste el término *anatomía* se asocia al estudio de la estructura del cuerpo humano y los animales, con un énfasis mínimo en la función de cada parte. A pesar de esta distinción, la anatomía y la fisiología no pueden ser separadas ya que la función de un tejido o de un órgano está íntimamente ligada a su estructura y la estructura de un organismo presumiblemente evoluciona para cumplir mejor su función. Por esta necesidad de apoyarse en la anatomía y porque incluye otras disciplinas como la física, la química y las matemáticas, la fisiología es una ciencia multidisciplinar.

Como se mencionó en el capítulo anterior, una de las características en que se basa la biometría para llevar a cabo la identificación de individuos es la característica física y para crear sistemas biométricos que realicen su labor de manera correcta y sin riesgos para el individuo es necesario estudiar la fisiología del elemento físico que va a ser utilizado para hacer la verificación de la identidad, lo cual se convierte en una medida de seguridad para el fabricante del sistema biométrico y para el individuo que se somete al uso del sistema.

II.3. Inteligencia Artificial.

Desde hace siglos el hombre ha intentado construir máquinas que realicen sus tareas más rutinarias o más peligrosas intentando imitar su comportamiento y el del resto de los seres vivos. Así, se diseñaron máquinas de calcular que ahorraban mucho tiempo al usuario y cometían menos errores, por ejemplo, el ábaco. Sin embargo, no es hasta la aparición del transistor y más concretamente de las computadoras cuando se empieza a hablar de máquinas inteligentes, por ello podemos definir Inteligencia Artificial como la rama de la informática que desarrolla procesos que imitan a la inteligencia de los seres vivos y su principal aplicación es la creación de máquinas para la automatización de tareas que requieran un comportamiento inteligente.

Los primeros desarrollos en Inteligencia artificial comenzaron a mediados de los años 50 con el trabajo de Alan Turing, por lo cual es considerado como el padre de la Inteligencia

Artificial. En 1950 Turing presentó el trabajo “Computing Machine and Intelligence” en el cual propone una prueba, conocida también como prueba de Turing (véase figura 2.2), la cual se fundamenta en la hipótesis positivista de que, si una máquina se comporta en todos los aspectos como inteligente, entonces debe ser inteligente. La prueba consiste en un desafío: la máquina debe hacerse pasar por humana en una conversación con una persona en una comunicación de texto, estilo chat. Al sujeto no se le avisa si está interactuando con una máquina o una persona. Si al término de dicha conversación la persona es incapaz de determinar si el interlocutor es humano o una máquina, entonces se considera que la máquina ha alcanzado un determinado nivel de madurez: es inteligente. Cabe mencionar que hoy en día no existe todavía ninguna máquina que pueda pasar esta prueba en una experiencia con método científico.

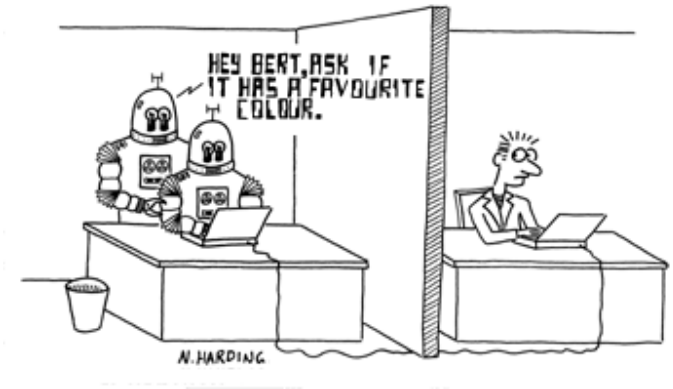


Figura 2.2 Prueba de Turing

Dentro de las diferentes áreas que abarca la Inteligencia Artificial la que más ha atraído a los investigadores en materia de biometría, es el aprendizaje de las máquinas. Por ejemplo para una máquina, la clasificación de rostros o el reconocimiento de letras son tareas mucho más difíciles que para un ser humano. La máquina necesita del aprendizaje pues debe adaptar los parámetros de un sistema, en este caso artificial, para obtener la respuesta deseada.

Que un sistema pueda mejorar su comportamiento sobre la base de la experiencia que recoge al efectuar una tarea repetitiva y que además, tenga una noción de lo que es un error y que pueda evitarlo, resulta en sistemas biométricos más eficaces y confiables.

II.4. Ciencias del Comportamiento.

Las ciencias sociales, conocidas también como las ciencias de la conducta humana, abarcan un grupo de disciplinas que estudian el comportamiento humano; entre estas disciplinas se encuentran la sociología, la psicología, la economía, la antropología y la pedagogía, cada una de las cuales aborda al ser humano desde una óptica que le permita comprenderlo para de esta forma llevar a cabo estudios de su comportamiento como

individuos, miembros de grupos, comunidades y organizaciones, de igual forma analizan cómo éstos han evolucionado biológica y culturalmente. Estas disciplinas también estudian cómo los seres humanos se organizan para producir lo que necesitan para sobrevivir, gobernarse, tomar decisiones, adaptarse y enfrentarse al ambiente físico que les rodea.

Las características del comportamiento de los individuos pueden ser medidas y por ende ser utilizadas por la biometría, específicamente por la biometría dinámica cuyas características se abordarán más a detalle en el capítulo III.

II.5. Modelo del proceso de identificación personal.

El modelo del proceso de identificación personal postula la existencia de tres indicadores de identidad que definen el proceso de identificación de un individuo, estos indicadores son: Posesión, es decir, lo que el individuo tiene, por ejemplo una clave de usuario. Conocimiento, este indicador de identidad se refiere a lo que el individuo sabe, por ejemplo una contraseña y por último Característica o bien "lo que el individuo es", es decir, la persona tiene una característica, ya sea física o conductual, por medio de la cual puede ser identificada, sin embargo, para que ésta pueda ser considerada un indicador de identidad debe cumplir con 4 requerimientos básicos, los cuales se describen a detalle a continuación.

II.5.1. Características de un Indicador de Identidad Biométrico.

Para que las características físicas y conductuales de un individuo puedan ser utilizadas como Indicadores de identidad deben cumplir con los siguientes requerimientos básicos:

- Universalidad: La palabra Universal define algo que comprende o es común a todos en su especie, en este caso, los seres humanos, por lo que el indicador de identidad seleccionado deberá estar presente en todos los individuos.
- Singularidad: La palabra singular hace referencia a algo que es único en su especie por lo que este requerimiento especifica que la existencia de dos personas con una característica idéntica tiene una probabilidad casi nula.
- Estabilidad: Algo que es estable se mantiene o permanece invariable e indefinidamente en el mismo estado, situación o lugar, por lo que el indicador de identificación elegido deberá estar presente a lo largo del tiempo y en condiciones ambientales diversas.
- Cuantificación: Cuantificar significa expresar de manera numérica una magnitud, por lo que este requerimiento nos dice que debe de ser posible medir o conocer la cantidad exacta que posee el indicador de identificación seleccionado.

Estos requerimientos nos sirven como criterio para descartar o aprobar alguna característica física o conductual como indicador biométrico, por ejemplo, en la tabla 2.1 se muestra el análisis de algunas características físicas bajo estos requerimientos:

Indicador	Universalidad	Singularidad	Estabilidad	Cuantificación
Cabello	No	No	No	Sí
Estatura	Sí	No	No	Sí
Distancia entre los ojos	Sí	No	Sí	Sí
Huella dactilar	Sí	Sí	Sí	Sí
Peso corporal	Sí	No	No	Sí
Geometría de la mano	Sí	Sí	Sí	Sí

Tabla 2.1 Análisis de Características Físicas.

Como se puede observar en la tabla, sólo dos de las características físicas que fueron seleccionadas cumplen con los cuatro requerimientos necesarios para ser consideradas como indicadores de identidad biométricos. Por lo tanto, y tomando en cuenta el resultado del análisis realizado en la tabla 2.1, podemos concluir que no todos los rasgos físicos pueden ser susceptibles de ser utilizados con el fin de identificar individuos, por lo cual es necesario que los fabricantes de tecnología biométrica lleven a cabo un estudio minucioso de la(s) característica(s) que fungirá como indicador de identidad y sobre la cual se producirá el sistema biométrico para que éste cumpla con su objetivo de manera adecuada.

II.5.2. Características de un sistema biométrico.

Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas.
Las características básicas que un sistema biométrico para identificación personal debe cumplir son: desempeño, aceptabilidad y fiabilidad. Las cuales apuntan a la obtención de un sistema biométrico con utilidad práctica.

a) Desempeño.

Esta característica se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación de individuos por parte del sistema biométrico. Otros factores que se toman en cuenta para evaluar el desempeño de éstos son los recursos tecnológicos invertidos en su fabricación, los costos asociados a la cantidad de sistemas requeridos por número de usuarios y el efecto de factores ambientales y/u operacionales sobre los sistemas. El objetivo de esta característica es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.

b) Aceptabilidad.

Indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Dicho sistema no debe representar peligro alguno para los usuarios por lo cual deberá ser un sistema de fácil uso y que inspire confianza a los usuarios finales.
Existen factores psicológicos que pueden afectar esta característica, por ejemplo, el reconocimiento de una retina requiere un contacto cercano de la persona con el dispositivo de reconocimiento, esto puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato".

c) Fiabilidad.

Esta característica refleja cuán difícil es burlar al sistema. Para que el sistema biométrico sea fiable cien por ciento debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz, prótesis de ojos, entre otros, para burlar la seguridad del sistema y obtener acceso al lugar deseado. Recientemente Investigadores de la Universidad de Clarkson (Postdam, N.Y.), con ayuda del financiamiento de instituciones gubernamentales de Estados Unidos como el Departamento de Defensa y la Fundación Nacional para las Ciencias, probaron que es posible engañar a este tipo de dispositivos con métodos relativamente sencillos. En su experimento, el equipo de investigadores creó 60 dedos falsos que lograron engañar a los dispositivos lectores de huellas digitales -y su software correspondiente- en 9 de cada 10 intentos. De acuerdo con los especialistas, las huellas dactilares falsas pueden ser extraídas de cadáveres o de personas vivas y ser moldeadas en plástico, o inclusive plastilina o gelatina. Los resultados de la investigación servirán para encontrar nuevos métodos para determinar si la característica bajo estudio corresponde o no a la de una persona viva y de esta forma impedir fraudes relacionados con los sistemas biométricos. Expertos en el área aseguran que otra forma de evitar fraudes en este tipo de sistemas es combinando los distintos rasgos biométricos que pueden ser utilizados como identificadores de identidad. Por ejemplo, se pueden fabricar sistemas que reconozcan la huella dactilar y una vez que ésta sea verificada se proceda al reconocimiento de la voz del usuario. Otro ejemplo podría ser la creación de sistemas que verifiquen la identidad de un individuo escaneando su iris o retina y que además requieran de una contraseña que al momento de ser introducida a través de un teclado será verificada y pasará por un análisis de velocidad de tecleo y presión ejercida sobre las teclas, es decir, se llevará a cabo el reconocimiento del patrón de tecleo del usuario. De esta forma se volverá mucho más difícil para los impostores poder falsificar todos los rasgos biométricos utilizados en este tipo de “sistemas combinados”. No obstante el elevado costo de este tipo de sistemas será una desventaja tanto para los fabricantes como para las empresas o particulares que decidan adquirirlos, esto debido a que la cantidad de hardware y software necesarios para que los sistemas operen como es deseado se verá incrementado y dependerá de la cantidad de características biométricas utilizadas.

Actualmente, algunos de los métodos que ya son empleados en este tipo de tecnologías son ingeniosos y usualmente más simples de lo que uno podría imaginar. Por ejemplo, un sistema basado en el reconocimiento del iris revisa patrones característicos en las manchas de éste, un sistema infrarrojo para verificar las venas de la mano detecta flujos de sangre caliente y lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos y los niveles de humedad en la piel. Sin embargo, y a pesar de los avances que en este campo se han desarrollado, aún falta mucha investigación para desarrollar un sistema biométrico cien por ciento fiable.

II.6. Arquitectura y Medidas de desempeño de un Sistema Biométrico.

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de un individuo, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos con los datos almacenados y el tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. La arquitectura de un sistema biométrico puede entenderse conceptualmente como dos módulos; el Módulo de Inscripción y el Módulo de Identificación (véase figura 2.3).

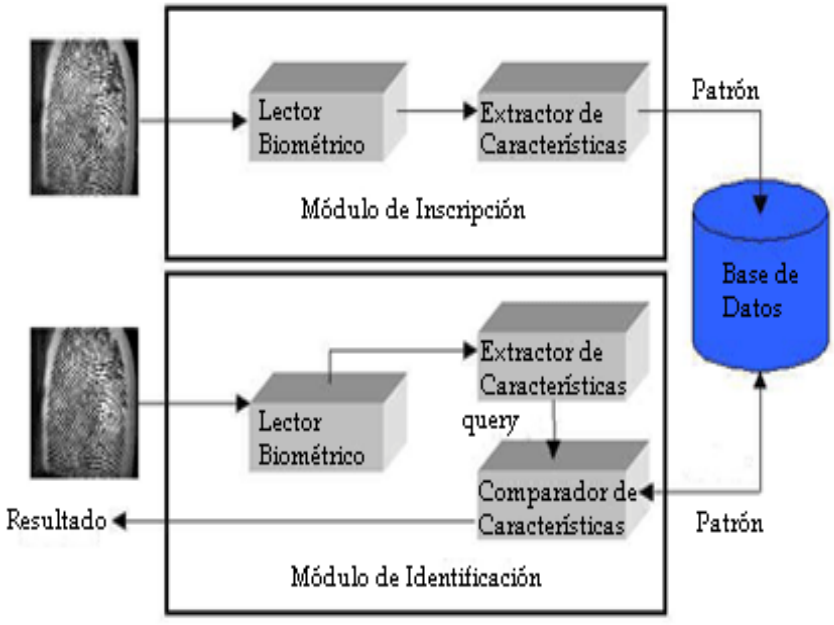


Figura 2.3 Arquitectura de Sistema Biométrico.

II.6.1. Módulo de Inscripción.

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar esta información con la que será proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características. El primero se encarga de adquirir datos relativos del indicador biométrico elegido y entregar una representación en formato digital de éstos. El segundo extrae, a partir de la salida del lector, características representativas del indicador. Durante este proceso de recopilación de datos, es en donde se presentan los primeros problemas. En primer lugar las muestras deben ser obtenidas mediante un sensor, por lo tanto, están sujetas a la calidad y características técnicas del sensor utilizado, lo que conlleva a que las características del sensor deberán ser estandarizadas, a fin de garantizar que las muestras obtenidas de un usuario en diferentes sistemas sean compatibles[1]. En cuanto al almacenamiento, existen varias formas de guardar los datos previamente recopilados y procesados, que al momento de ser almacenados reciben el nombre de *patrón (template)*. La organización de la estructura de los datos debe ser flexible, permitiendo su reestructuración, si fuese necesario. De esta forma es posible definir algunos sistemas de almacenamiento, para diferentes tipos de medidas biométricas, dependiendo de sus características particulares:

1. Sistema protegido dentro del dispositivo biométrico.
2. Base de datos convencional.
3. Token portátil, por ejemplo una tarjeta inteligente.

II.6.2. Módulo de Identificación.

El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo, en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato del patrón. La representación resultante se denomina *query* (consulta) y es enviada al comparador de *características* que confronta a éste con uno o varios patrones para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de *fase de inscripción*, mientras que los procesos realizados por el módulo de identificación reciben la denominación de *fase operacional*.

[1] La calidad de los sensores biométricos se encuentra se encuentra en proceso de estandarización por parte del Instituto Nacional de Estándares y Tecnología (NIST).

II.6.3. Medidas de Desempeño.

La información provista por los patrones permite particionar su base de datos de acuerdo con la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las clases así generadas permiten reducir el rango de búsqueda de algún patrón en la base de datos. Sin embargo, los patrones pertenecientes a una misma clase también presentarán diferencias conocidas como *variaciones intraclase*. Las variaciones intraclase implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

1. Una persona autorizada es aceptada.
2. Una persona autorizada es rechazada.
3. Un impostor es aceptado.
4. Un impostor es rechazado.

Debido a esto la efectividad de un sistema biométrico se mide en términos de los siguientes índices: Tasa de falsa aceptación (False acceptance Rate o FAR), Tasa de Falso Rechazo (False Rejection Rate o FRR).

a) Tasa de falsa aceptación: Este parámetro hace referencia a la probabilidad de que un usuario no autorizado sea aceptado.
b) Tasa de falso rechazo: El parámetro hace referencia a la probabilidad de que un usuario que está autorizado sea rechazado a la hora de intentar acceder al sistema, este parámetro se encuentra fuertemente afectado por las condiciones del proceso de captura.

La FAR y la FRR son funciones del grado de seguridad deseado que pueden transformarse en los demás índices cambiando cierto parámetro. Usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa. El grado de seguridad deseado se define mediante el umbral de aceptación o un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

En la figura 2.4 se muestra una gráfica típica de la FRR y la FAR como funciones del umbral de aceptación u. En esta figura puede apreciarse un umbral de aceptación particular, denotado por u*, donde la FRR y la FAR toman el mismo valor. Este valor recibe el nombre de tasa de error de intersección (cross-over error rate*)* y puede ser utilizado como medida única para caracterizar el grado de seguridad de un sistema biométrico. En la práctica, sin embargo, es usual expresar los requerimientos de desempeño del sistema, tanto para verificación como para identificación, mediante la FAR. Usualmente se elige un umbral de aceptación por debajo de u* con el objeto de reducir la FAR, en deterioro del aumento de la FRR.

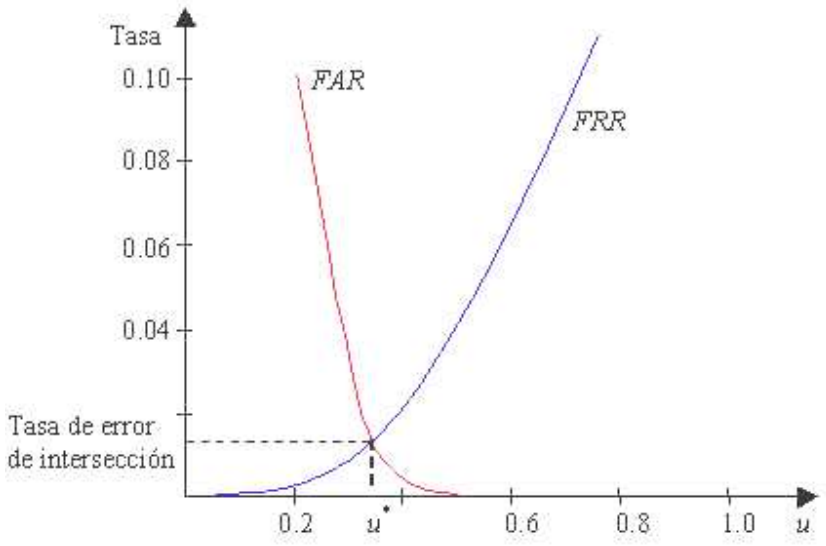


Figura 2.4 Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación u para un sistema biométrico.

Cabe mencionar que no se encontró ningún tipo de información en donde se exponga si los índices mediante los cuales se mide la efectividad de los sistemas biométricos, es decir FAR y FRR, tienen relación con los niveles de seguridad propuestos por algún estándar vigente, sin embargo se sabe que el nivel de seguridad de un sistema biométrico puede ser programado por el administrador del sistema de dos formas según las necesidades de la empresa o del lugar donde se haga uso de esta tecnología:

- La primera forma es incrementar el valor del umbral de aceptación (u) para que el acceso a personas no autorizadas sea más difícil, es decir, disminuye FAR.

- La segunda forma es disminuir el valor de u para que el acceso a personas autorizadas sea más fácil, es decir, disminuye FRR, no obstante esta acción aumenta el riesgo de falsa aceptación (FAR).

CAPÍTULO III

Clasificación de los sistemas Biométricos.

III.1 Por su tipo.

Como se ha mencionado ya en varias ocasiones, la biometría es el estudio de métodos automáticos para el reconocimiento único de individuos basados en rasgos conductuales o físicos intrínsecos y dependiendo del tipo de característica que se utilice para llevar a cabo dicha identificación es que la biometría se divide en dos grandes tipos: Biometría Estática y Biometría Dinámica.

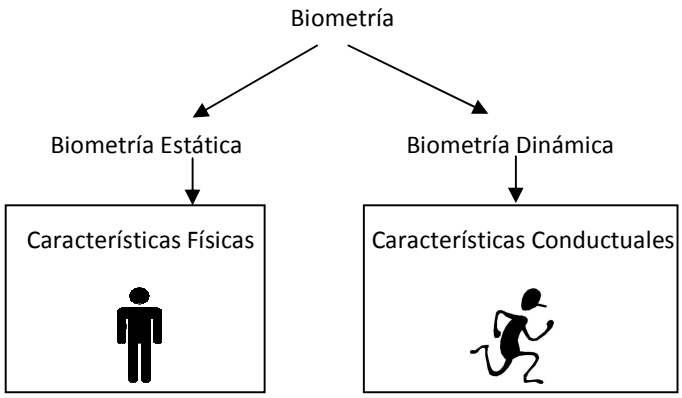


Figura 3.1 Clasificación de la biometría por su tipo.

Como se puede observar en la figura 3.1, la medición de las características físicas de un individuo corresponde a la *Biometría Estática*. Los principales estudios y aplicaciones de esta rama de la biometría están basados en los sistemas biométricos de huellas dactilares, geometría de la mano, análisis de iris y retina, reconocimiento facial.
Por el contrario, la medición de los rasgos de comportamiento de un individuo forman parte de la *Biometría Dinámica* y dentro de esta rama de la biometría los principales estudios y aplicaciones están basados en los sistemas de reconocimiento de voz y firma manuscrita principalmente.

III.2 Por su tecnología.

La tecnología biométrica es el desarrollo de aplicaciones (sistemas biométricos) que permiten llevar a cabo de manera automatizada la identificación y verificación de la identidad de los individuos. A continuación se describen de manera general las tecnologías biométricas con más presencia en el mercado.

III.2.1. Reconocimiento de Huella dactilar.

El reconocimiento de huella dactilar (véase figura 3.2) es el método de identificación biométrica por excelencia debido a que es fácil de adquirir, fácil de usar y por ende goza de gran aceptación por parte de los usuarios. Como se describió en el Capítulo I, el uso de

huellas dactilares para establecer la identidad de una persona tuvo su origen a mediados del siglo XIX, siendo pionero en esta área sir William Herschel.

Figura 3.2 Reconocimiento de huella dactilar.

La huella dactilar es una característica física única que distingue a todos los seres humanos y la ciencia que se encarga de su estudio se conoce como *Dactiloscopia*, que viene de los vocablos griegos *daktilos* (dedos) y *skopein* (examen o estudio). Este nombre fue inventado por el doctor Francisco Latzina en sustitución al dado en 1892 por Sir Francis Galtón (Icnofalangometría). Todos los sistemas dactiloscópicos se basan en tres principios fundamentales:

Φ Perennidad: Gracias al fisiólogo checo Juan Evangelista Purkinje se sabe que las huellas dactilares se manifiestan a partir del sexto mes del desarrollo del embrión y que están presentes a lo largo de toda la vida de los seres humanos y hasta la descomposición del cadáver.

Φ Inmutabilidad: Las huellas dactilares no se ven afectadas en sus características por el desarrollo físico de los individuos ni por enfermedades de ningún tipo y en caso de que llegase a presentarse un desgaste involuntario (por ejemplo una herida o quemadura), el tejido epidérmico que la conforma es capaz de regenerase tomando su forma original en un periodo de 15 días.

Φ Diversidad Infinita: Las huellas dactilares son únicas e irrepetibles, cada ser humano posee huellas dactilares con características individuales. Es un error común pensar que los gemelos idénticos no cumplen con este principio, sin embargo, las huellas dactilares no se desarrollan debido a un proceso genético sino a un proceso aleatorio por lo que no existe ningún tipo de correlación entre gemelos idénticos o individuos de una misma familia.

A simple vista toda persona puede observar que la piel no es enteramente lisa o uniforme, sino que está cubierta de rugosidades, protuberancias y depresiones en la dermis, a continuación se describen estas rugosidades:

a) Papilas: Son las pequeñas protuberancias que nacen en la dermis y sobresalen completamente en la epidermis, sus formas son muy variadas; unas son cónicas, otras hemisféricas y otras piramidales o simulando verrugas. El número de papilas agrupadas en cada milímetro cuadrado se calcula que es de 36 y su tamaño es de 55 a 225 milésimos de milímetro de altura.

b) Crestas: Las crestas son los bordes sobresalientes de la piel que están formados por una sucesión de papilas, estos bordes siguen las sinuosidades de los surcos en todas direcciones y forman una infinidad de figuras en las yemas de los dedos, son más amplios en su base que en la cúspide, dan el aspecto de una montaña en miniatura y reciben el nombre de *crestas papilares.*

c) Surcos: Se les da el nombre de surcos a los espacios hundidos los que se encuentran entre papila y papila. También se les conoce con el nombre de surcos interpapilares debido a que al entintar los dedos, la tinta no cubre completamente las yemas, por ello al hacer la impresión de las huellas sobre cualquier superficie plana quedan espacios en blanco.

d) Poros: Los poros son los pequeños orificios que se encuentran situados en la cúspide de las crestas papilares o cerca de su vértice, tienen la función de segregar el sudor. Estos poros tienen diferentes formas que pueden ser circulares, ovoidales, triangulares, etc.

Los dibujos o figuras formadas por las *crestas papilares* reciben el nombre de *dactilogramas* (véase figura 3.3) palabra que deriva de los vocablos griegos; *daktylos* (dedos) y *grammas* (escrito). Se denominan dactilogramas papilares si provienen de los dedos de la mano, plantares si provienen de la planta del pie y palmares cuando provienen de la palma de la mano. Los dactilogramas se pueden clasificar de tres formas:

Φ Dactilograma natural: es el que está en la yema del dedo, formado por las crestas papilares de forma natural.

Φ Dactilograma artificial: es el dibujo que aparece como resultado al entintar un dactilograma natural e imprimirlo en una zona idónea.

Φ Dactilograma latente: es la huella dejada por cualquier dactilograma natural al tocar un objeto o superficie. Este dactilograma queda marcado, pero es invisible. Para su revelación requiere la aplicación de un reactivo adecuado.

Figura 3.3 Crestas papilares de las yemas de los dedos.

De igual forma un dactilograma se puede dividir en tres partes que se conocen como: *sistemas dactilares* los cuales son el Sistema basilar, el Sistema marginal y el Sistema nuclear (véase figura 3.4); donde el sistema basilar es la zona que se encuentra entre la segunda y tercera falange de los dedos, excepto por el dedo pulgar, donde la zona se ubica entre la primera y la segunda falange, normalmente las crestas de esta zona son horizontales. El sistema marginal es la zona más exterior del dactilograma, normalmente corresponde a la zona de la punta de los dedos y los bordes del mismo; sus crestas suelen ser angulosas. Finalmente el sistema nuclear es la zona comprendida entre el sistema basilar y el marginal, contiene el centro de la impresión dactilar (núcleo) y la mayor parte de los puntos característicos del dactilograma.

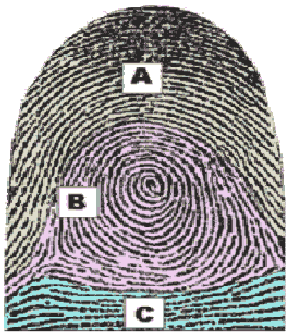


Figura 3.4 A) Sistema Marginal, B) Sistema Nuclear, C) Sistema Basilar.

Todos los dactilogramas coinciden en el hecho de que las crestas papilares no describen formas aleatorias, sino que se agrupan hasta llegar a constituir sistemas definidos por la uniformidad de su orientación y figura. Se pueden distinguir cuatro grupos o clases distintas de configuraciones dérmicas según la denominada *Clasificación de Henry*[1], pero antes debemos estudiar dos singularidades presentes en algunas huellas denominadas *Núcleo* (Core) *y Delta* (véase figura 3.5). El núcleo responde al punto localizado en la zona

[1] Henry Faulds, médico y misionero escocés, pionero de la identificación de personas a través de las huellas dactilares que en 1880 publicó un ensayo sobre el comportamiento de las huellas dactilares y realizó una propuesta a Scotland Yard sobre un sistema de clasificación de las crestas papilares que conforman los dactilogramas donde se pueden distinguir cuatro grupos o clases distintas de configuraciones dérmicas. El sistema creado por Faulds también es conocido como Sistema Bengalés o Sistema Galton - Henry.

central de la huella, donde una de las crestas cambia bruscamente su dirección y describe el ángulo de 180°, regresa, por lo tanto, a la posición de origen. Este punto se utiliza como punto de referencia a partir del cual se cuentan el número de crestas a considerar en un análisis dactiloscópico concreto.
El Delta es un punto característico del dibujo papilar de algunas huellas que pueden asemejarse a la letra griega delta (Δ), está formado por la aproximación o fusión de las crestas existentes en la frontera entre las zonas marginal, basilar y nuclear de la huella. La importancia de este punto radica en que la zona en donde se ubica aparecen muchos puntos característicos.

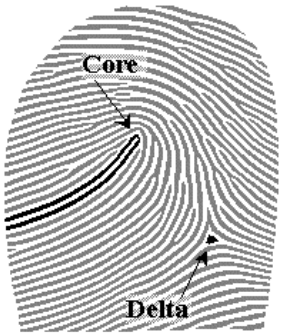


Figura 3.5 Puntos singulares de la huella dactilar.

A continuación se detallan las seis clases propias de la clasificación de Henry:

a) Arco: Este dactilograma es uno de los tipos fundamentales, carece de puntos delta y de núcleo. Se caracteriza porque en un comienzo las crestas son casi rectas y paulatinamente se van arqueando para dar forma aproximada de medio círculo. (véase figura 3.6).

Figura 3.6 Arco.

b) Presillas Internas: Se caracterizan porque las crestas que forman su núcleo nacen en el costado izquierdo del dibujo y hacen su recorrido a la derecha, para luego dar vuelta sobre sí mismas y regresar al mismo punto de partida. Cuentan con un punto Delta que como se puede observar en la figura 3.7 se ubica del lado derecho del observador.

Figura 3.7 Presilla Interna.

c) Presillas Externas: Al igual que las presillas Internas, cuentan con un punto Delta, pero éste se ubica del lado izquierdo del observador. Las crestas papilares que forman el núcleo nacen a la derecha y su recorrido es a la izquierda para dar vuelta sobre sí mismas y regresar al mismo punto de partida (véase figura 3.8).

Figura 3.8 Presilla Externa.

d) Verticilo: Se denomina verticilo debido a que sus dibujos en muchos casos son similares a las flores; su característica más importante es que cuenta con dos puntos Delta, uno del lado derecho y otro del lado izquierdo, sus núcleo puede adoptar formas circulares, elípticas y espirales (véase figura 3.9). Se pueden encontrar verticilos con tres deltas llamados también trideltos, aunque esto sucede con poca frecuencia.

Figura 3.9 Verticilo.

III.2.1.1. Adquisición de la Huella dactilar.

Existen dos métodos de adquisición de huellas dactilares: método *off-line* y el método *on-line*. El primer método obtiene la huella digitalizada con una resolución espacial de 500dpi (dots per inch: puntos por pulgada) y a 256 niveles de profundidad de gris, esto según recomendaciones del FBI mediante el escaneo de una huella impresa en papel obtenido a partir de la operación tradicional de calcado del dedo tintado sobre papel satinado. Esta metodología de funcionamiento requiere de un costo importante de tiempo y es la que suele usarse en aplicaciones criminalistas. En cambio el segundo método se realiza en tiempo real mediante el escaneo directo de la huella a través del uso de escáneres tipo *inkless* que se describen en el Apéndice A. Esta metodología es la que frecuentemente se utiliza en aplicaciones civiles.

Tras la captura de la huella se realizará una valoración cualitativa de la misma, el resultado de la cual será:

a) Huella apta para ser procesada.
b) Huella recuperable mediante técnicas de preprocesado digital de imagen.
c) Huella inutilizable para debido a la baja calidad de la adquisición.

III.2.1.2. Procesamiento de la Huella Dactilar.

Los pasos para el procesamiento de la huella dactilar por un sistema automatizado de identificación de impresiones dactilares son:

1. **Mejora de la Imagen:** Este proceso consiste en eliminar las zonas confusas de la imagen original (ruido) dejando sólo zonas con información de máxima fiabilidad.
2. **Binarización:** El objetivo de esta etapa es pasar la imagen original en tonos de gris a blanco y negro, reconstruyendo posibles cortes y mejorando la calidad global de la imagen.
3. **Adelgazamiento:** Con este proceso todas las crestas de las líneas dactilares tienen el mismo grosor (1 píxel), haciendo que los puntos característicos de la huella dactilar se puedan identificar con más facilidad.
4. **Extracción de puntos característicos:** A partir de la imagen adelgazada y el sistema es capaz de detectar y extraer la posición exacta de los puntos característicos. Dentro de esta etapa cabe destacar:
    a) **Construcción de un índice o vector:** Este es el proceso final que mediante algoritmos matemáticos completa la creación de un índice matemático, el cual constituye la esencia de la huella dactilar analizada, según las características consideradas, almacenándolo en forma de fichero (este fichero ocupa aproximadamente 300 bytes).

b) **Identificación y Verificación:** Una vez que se tienen el índice o vector de muchas huellas, el sistema es capaz de realizar búsquedas 1:1 para verificar la identidad de una persona o 1:N para identificarla.

La extracción de puntos característicos es por lo tanto el proceso final que completa la obtención de la plantilla de la huella o patrón biométrico dactilar. La cantidad mínima de puntos característicos necesarios para proceder a comparaciones eficaces entre imágenes dactilares es de 15. La extracción de puntos característicos es un área en la que la investigación es continua y al día de hoy se puede llevar a cabo con diversas técnicas:

Φ **Extracción de puntos característicos desde la imagen de la huella.** En esta técnica se apuesta por hacer un preprocesado de la huella antes de detectar las características de la misma. Una vez hecho esto se buscan los patrones a identificar sobre la huella preprocesada, en la cual la anchura de las crestas es de un píxel. El preprocesamiento de la huella hace que el sistema de extracción pueda trabajar con huellas con un amplio rango de calidades. Esta es la técnica más clásica y típica dentro de la extracción de puntos característicos de huella dactilar.

Φ **Extracción de los puntos característicos mediante un banco de filtros de Gabor.** Esta es una técnica bastante novedosa y utiliza una extracción de los puntos característicos de las huellas dactilares basada en un banco de filtros de Gabor. Esta técnica es usada para capturar la información útil en las bandas de los canales de la imagen y descomponer la información en componentes ortogonales en términos de frecuencias espaciales. La técnica presenta buenas características de precisión, pero en cuanto a la velocidad de extracción presenta resultados pobres, siempre peores que las técnicas de extracción más clásicas.

Φ **Extracción de los puntos característicos sobre la propia imagen de la huella en escala de grises.** En esta técnica se caracteriza por realizar la extracción sobre la propia huella y no sobre la imagen adelgazada o mejorada de la misma. Esto presenta muchos inconvenientes y hace que la extracción sea más lenta, inexacta y dependiente de la calidad de la huella. Además trabajando directamente sobre la huella en escala de grises se detectarán un gran número de puntos característicos falsos y habrá otros muchos auténticos que no se detecten. Debido a estos inconvenientes la técnica no es muy utilizada.

III.2.2. Reconocimiento de Iris y retina.

La utilización del ojo humano en la identificación de personas ha dado lugar a dos técnicas biométricas diferentes: una basada en las características del iris ocular y otra que utiliza las características distintivas de la retina. Únicamente tienen en común que se sirven de un mismo órgano, el ojo humano, sin embargo, en numerosas ocasiones se suele confundir uno con otro y ambas se consideran como una única técnica denominada

biometría del ojo, por lo tanto es importante resaltar que el iris y la retina oculares dan lugar a dos tipos de sistemas biométricos completamente diferentes, tanto en los métodos de captura de imagen y las técnicas de extracción de características como en los métodos de comparación.

El ojo humano es un órgano fotorreceptor, cuya función consiste en recibir los rayos luminosos procedentes de los objetos presentes en el mundo exterior y transformarlos en impulsos eléctricos que son conducidos al centro nervioso de la visión en el cerebro. La estructura del ojo se puede observar en la figura 3.10. El sistema óptico está formado básicamente de tres capas: la capa externa, la capa media y la capa interna.

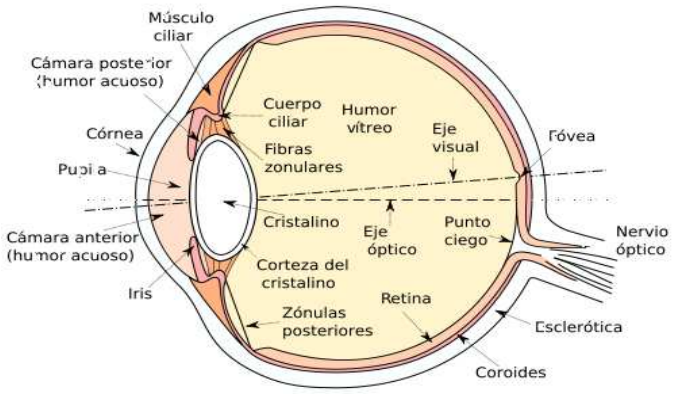


Figura 3.10 Estructura del globo ocular.

La capa externa está compuesta de la córnea, la esclerótica y el limbo. La *esclerótica* es una membrana opaca, densa y fibrosa de color blanco cuya función es la de dar forma al globo ocular y proteger a los elementos más internos. Cubre aproximadamente las cuatro quintas partes del ojo. La esclerótica presenta dos orificios principales, uno posterior por donde salen las fibras del nervio óptico, y otro anterior donde se localiza la córnea. Los seis músculos de la esclerótica (véase figura 3.11) mueven el globo ocular, ambos ojos se mueven de forma coordinada en la misma dirección. Estos músculos son: músculo oblicuo superior, músculo oblicuo inferior, músculo recto lateral, músculo recto inferior, músculo recto medio y músculo recto superior. La *córnea* es una membrana resistente a través de la cual la luz penetra en el interior del ojo. Detrás de la córnea hay una cámara llena de fluido claro y húmedo (humor acuoso) que separa la córnea del cristalino. La córnea se encuentra unida a la esclerótica por medio del limbo y se puede considerar como una lente externa que posee el mayor poder refractivo dentro del ojo. El *limbo* es la zona de transición entre la cornea y la esclerótica que contiene las estructuras responsables del drenaje de liquido del ojo (humor acuoso).

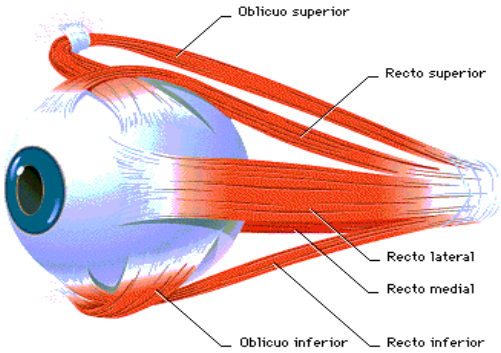


Figura 3.11 Músculos de la esclerótica.

La capa media, también denominada *tracto úveal* o simplemente *úvea*, está formado por el iris, el cuerpo ciliar y la coroides. El *iris*, visible a través de la cornea, es la parte del tracto úveal más accesible para una inspección directa. Es una estructura pigmentada que contiene los *músculos esfínter* y *dilatador del iris*, que actúan como diafragma ocular. El iris se encuentra situado entre la córnea y el cristalino y presenta una abertura en su parte central denominada *pupila*; El tamaño de la pupila depende de un músculo que rodea sus bordes, aumentando o disminuyendo cuando se contrae o se relaja, controlando la cantidad de luz que entra en el ojo. El *cuerpo ciliar* es adyacente y continuo al iris, se puede visualizar como un anillo. Contiene los *músculos ciliares* que hacen posible la acomodación del cristalino cuando los ojos se enfocan en algo. De igual forma el cuerpo ciliar contiene *la porción epitelial* que se encarga de realizar la unión con la retina y la producción del humor acuoso.
La *coroides* es una capa de vasos sanguíneos que se encuentra entre la esclerótica y la retina y que suministra de oxígeno y nutrientes al globo ocular.

La capa interna del ojo se denomina *retina* (véase la figura 3.12); es la capa cuya función es transformar la luz en un impulso nervioso que será dirigido al cerebro. En la superficie de la retina se pueden observar diversas estructuras:

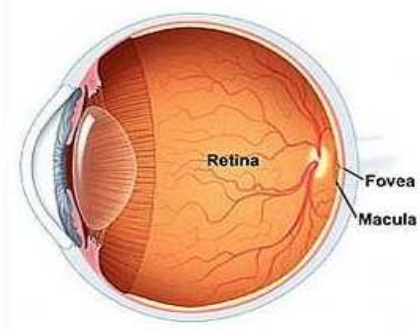


Figura 3.12 Retina

Φ Ora Serrata: Es el límite de la retina. Existe una ora serrata nasal o medial y una ora serrata lateral o temporal.

Φ Fóvea: Es una pequeña depresión en la retina que se encuentra en el centro de la *mácula lútea* que es una mancha amarilla ovalada en el centro de la retina que permite al ojo percibir detalles finos, es decir, otorga la agudeza visual. La fóvea es el área donde se enfocan los rayos luminosos y se encuentra especialmente capacitada para la visión aguda y detallada, no posee bastones sino sólo conos que son los responsables de la percepción de colores. La visión nocturna corresponde a la periferia de la retina que es donde abundan los bastones. Un objeto que el ojo enfoca se fija siempre de manera tal que su reflejo se ubique exactamente justo en la fóvea.

Φ Área central de la retina**:** Es la porción de la retina que rodea a la fóvea y donde se produce la mayor fotorrecepción.

Φ Área periférica de la retina: Los elementos de la retina son de menor número, de mayor tamaño y distribuidos menos regularmente. Tiene menos capacidad de fotorrecepción.

Φ Punto ciego: Éste es encontrado en la parte posterior del globo ocular, se le denomina así por el orificio o perforación que se encuentra en esa región, por el cual el nervio óptico llega al ojo atravesando así la membrana esclerótica, la coroides y finalmente la retina.

En el interior del glóbulo ocular se encuentra el *cristalino* que es una lente biconvexa y carente de nervios que está situado detrás del iris y delante del humor vítreo. Su propósito principal consiste en permitir enfocar objetos situados a diferentes distancias Este objetivo se consigue mediante un aumento de su curvatura y de su espesor, proceso que se denomina acomodación. El cristalino se caracteriza por su alta concentración en proteínas, que le confieren un índice de refracción más elevado que los fluidos que lo rodean. Este hecho es el que le otorga su capacidad para refractar la luz, ayudando a la córnea a formar las imágenes sobre la retina. A medida que la edad del sujeto aumenta, el cristalino va perdiendo progresivamente su capacidad para acomodar. Este fenómeno se conoce como presbicia o vista cansada y afecta a la totalidad de la población a partir de los cincuenta años, exigiendo el uso de anteojos para enfocar objetos cercanos.

La parte del globo ocular que se encuentra en contacto con el exterior, la córnea y la parte de la esclerótica se encuentra a su vez protegidos por los *párpados* y por las segregaciones de las glándulas lagrimales. Tanto la superficie interior de los párpados como la cara anterior de la esclerótica están tapizados por *la conjuntiva* que además ayuda a lubricar el globo ocular, produciendo mucosidad y lágrimas, aunque éstas en una cantidad menor que las glándulas lagrimales.

III.2.2.1 Reconocimiento del Iris Ocular.

En los últimos años la identificación basada en el patrón del iris ocular ha experimentado un gran auge debido a los excelentes resultados obtenidos y al gran interés que están

mostrando algunos sectores económicos para incorporar dicha técnica a sus sistemas de identificación. Algunas de las características que hacen del iris una aplicación potencial para la identificación biométrica son su estabilidad frente a los cambios originados por accidentes, esto debido a la protección que le confiere la córnea. El iris presenta pequeñas variaciones en su apertura tanto con cambios de iluminación como con iluminación fija, esta característica proporciona un mecanismo sencillo para detectar si el sujeto que está haciendo uso de esta tecnología está vivo. Otra característica importante es que este tipo de tecnología adquiere los datos necesarios para su funcionamiento de forma no invasiva para el usuario. Todas estas características se vuelven importantes a la hora de estudiar la viabilidad de la técnica biométrica, sin embargo, falta la característica fundamental: la *unicidad*; según varios estudios, en el patrón del iris hay más información que identifica unívocamente a una persona que en una huella dactilar, incluso los dos ojos de una persona poseen patrones distintos, característica muy importante que debe ser considerada en el sistema pues el ojo del cual se tome la imagen que servirá como patrón deberá ser el mismo que se utilice para conceder el acceso. Con todo esto se puede asegurar que esta técnica presenta una unicidad extremadamente alta lo que llevaría a unas tasas de falsa aceptación nulas lo que garantiza la viabilidad de esta técnica biométrica.

La idea de utilizar el patrón del iris para identificar a las personas fue propuesta inicialmente en 1936 por el oftalmólogo Frank Burch, pero no sería hasta 1987 que se patentó la idea y esto fue hecho por los oftalmólogos Leonard Flom y Aran Safir. Sin embargo, su incapacidad para poder desarrollar el sistema los empujó a contactar con el profesor John G. Daugman de la Universidad de Harvard para que fuera éste quien desarrollara los algoritmos necesarios para realizar el reconocimiento biométrico a través del patrón del iris. Estos algoritmos fueron patentados en 1994 y son la base de todos los sistemas de reconocimiento por iris existentes.

Flom, Safir y Daugman fundaron la compañía *IriScan Corp*, empresa que tenía en su poder la patente y que se encargaría de licenciarla a otras compañías. Una de esas compañías es *Sensar Corp*, no obstante la situación económica mundial llevó a estas dos compañías a conseguir su viabilidad económica mediante su fusión, creando así en el año 2000 la compañía *Iridian Technologies*[2] encargada de licenciar las patentes y de promover el desarrollo de productos y sistemas.

III.2.2.1.1 Captura de la Imagen del Iris.

Como ya se ha mencionado, la imagen del iris es accesible desde el exterior a través de la córnea y para su captura se pueden plantear dos posibilidades: el uso de cámaras digitales o el uso de cámaras de video. Al momento de plantear el sistema de captura se deben tener en cuenta los siguientes parámetros:

[2] www.iridiantech.com

a) La resolución de la cámara que debe ser los suficientemente alta para capturar la imagen del iris de manera correcta.
b) El usuario debe de colocarse lo suficientemente cerca del dispositivo de captura para obtener una imagen apropiada, sin embargo, este acercamiento no debe representar una amenaza para el individuo.
c) La captación de la imagen a la distancia elegida no debe suponer una deformación de la imagen capturada.

Una vez superada la fase de elección del dispositivo de captura, se debe diseñar el entorno de captura, el cual radica en tratar el tema de la iluminación que debe recibir el ojo para obtener una fotografía de calidad. No obstante en esta fase se pueden presentar problemas debido a la alta capacidad de reflexión de la córnea que al ser una superficie lisa y bien lubricada refleja todo rayo de luz que le llega, es por ello se sugiere que se trabaje en el rango infrarrojo pues de esta forma la iluminación necesaria para obtener la imagen del iris no molesta al usuario y las imágenes obtenidas no son dependientes del color.

La detección del fraude (por ejemplo si se presenta una fotografía o un ojo de plástico, u otro material, con el iris pintado) se puede realizar de forma sencilla capturando dos fotogramas consecutivos de la imagen, y comparar la dilatación de la pupila, que deber ser distinta. También se pueden forzar cambios controlados de la iluminación para analizar la respuesta de la pupila a dichos cambios.

III.2.2.1.2 Preprocesado del Iris.

La etapa de preprocesado tiene una gran importancia en esta técnica ya que la labor de adaptar la señal a los requisitos del bloque de extracción de características conlleva:

- La localización del iris dentro de la imagen.
- La detección de los bordes del iris. En este caso hay que tratar con dos bordes: el exterior (frontera con la esclerótica) y el interior (límite de la pupila).
- Eliminación de las partes no deseadas.
- Compensación del tamaño del iris, esto debido a la distancia del sujeto respecto al objetivo y de la dilatación o contracción de la pupila.
- Adaptación de la imagen a la técnica de extracción de características a realizar.

El primer paso en el preprocesado, en los casos en que la imagen sea tomada con una cámara en color, es una conversión a blanco y negro. Después independientemente del tipo de imagen capturada, se realizará un estiramiento del histograma[3] de la imagen para aumentar el contraste. La pupila del ojo aparece en el histograma como un pico bien

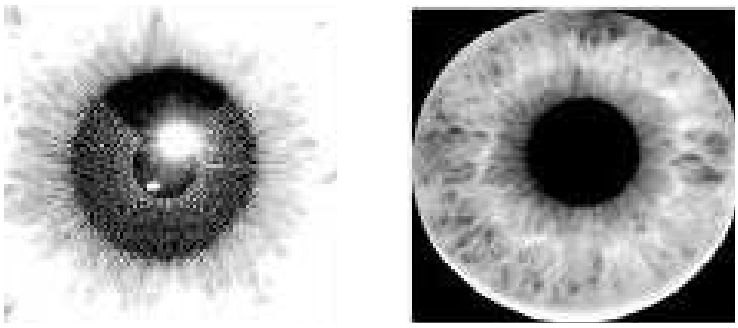
[3] El histograma de una imagen es una herramienta visual que entrega información sobre la estadística de la señal, es un parámetro inestable para el reconocimiento automático de formas y, en general, para el análisis de imágenes.

marcado en los valores bajos de intensidad de gris (dado que la pupila es negra). Una vez realizado esto, se procederá a la detección del borde externo del iris (el límite entre el iris y la esclerótica) mediante un algoritmo iterativo de búsqueda del máximo gradiente de intensidad a los largo de una circunferencia. El centro de dicha circunferencia, así como su radio, irán variando de tal forma que se recorra gran parte de la superficie de la imagen, obteniendo así el máximo.

Una vez detectado el borde externo (véase figura 3.13), se aplican las transformaciones necesarias al centro y el valor del borde para obtener los correspondientes en la imagen original. Se recorta la imagen original formando un cuadrado que englobe al iris detectado y se eliminan aquellos puntos que quedan fuera de la circunferencia que enmarca al iris. Una vez realizado esto, se vuelve a hacer una copia de dicha imagen, se eliminan los puntos de sobre-exposición y se estira el histograma. Esta última operación va a permitir aprovechar todo el rango dinámico de intensidad en el iris, de forma que, aunque éste sea oscuro, se va a poder distinguir de la pupila a la hora de detectar el borde interno.

Figura 3.13 Detección del borde externo del iris.

Para detectar el borde interno se podría pensar en utilizar el mismo centro, sin embargo, la pupila no es concéntrica con el iris por lo que hay que volver a realizar una nueva búsqueda del centro. El resultado de esta nueva búsqueda es el centro de la pupila, el radio de ésta y su situación dentro del borde externo del iris. Para obtener este centro, se aplica de nueva cuenta el proceso utilizado para detectar el borde externo sobre la imagen obtenida en el paso anterior (véase figura 3.13). Los puntos comprendidos dentro de la circunferencia definida se anulan en la imagen resultante de la detección del borde externo, y se vuelve a realizar un estiramiento del histograma con lo que se obtiene el iris aislado del resto de la imagen (véase figura 3.14 b)).



a) b)

Figura 3.14 a) Detección del borde Interno del Iris; b) Imagen del iris aislado resultante.

III.2.2.1.3 Adaptación del Iris Detectado.

Una vez aislado el iris de toda la imagen hay que considerar las variaciones debidas al tamaño del mismo y a la dilatación de la pupila. Para simplificar el algoritmo de extracción de características se va a realizar una transformación de forma que en los datos que se le van a pasar a dicho bloque estén suprimidos los conos superior e inferior y que el tamaño de los datos sea el mismo independientemente del tamaño del iris y de la pupila. Para esto se realiza un muestreo tanto en radio como en ángulo de la imagen del iris obtenida.

De una forma visual, la transformación realizada se ilustra en la figura 3.15 donde se puede observar que cada uno de los conos laterales, mediante muestreo de radio y ángulo, se convierte en una imagen cuadrada, cuyas columnas indicarán fracciones del radio, mientras que las filas serán incrementos de ángulo. Conectando ambas imágenes, se obtiene la matriz rectangular que se utilizará en el bloque de extracción de características.

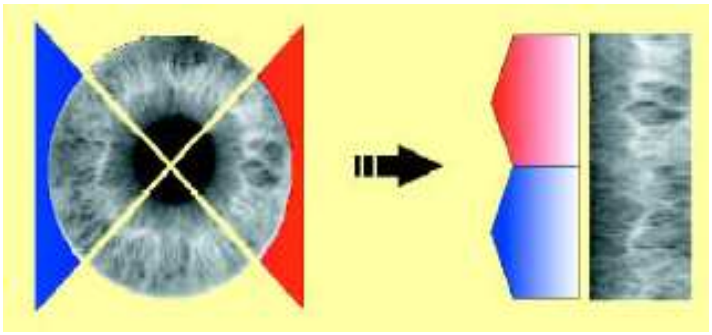


Figura 3.15 Transformación efectuada al iris aislado.

Debido a que el muestreo se realiza en función de la separación entre el borde externo y el borde interno, siempre se seleccionará el mismo número de punto y, por tanto, la

matriz resultante será siempre del mismo tamaño, lo cual facilitará el tratamiento del siguiente bloque.

Una vez realizado el preprocesado de la imagen, y obtenida una matriz rectangular de datos que reflejan un muestreo de la intensidad de la imagen del iris en los conos, se entra en el bloque de extracción de características. Existen varias técnicas para extraer las características de la imagen del iris como son la Transformada de Wavelet, La Extracción por Circunferencia y Los Filtros de Gabor, siendo ésta última la más utilizada.

III.2.2.2. Identificación por escaneo de Retina.

La identificación biométrica mediante retina se basa en la utilización del patrón de los vasos sanguíneos contenidos en la retina (véase figura 3.16). El patrón de la distribución de los vasos sanguíneos que emanan del nervio óptico y aparecen dispersos en la retina es, indudablemente una fuente de información biométrica altamente distintiva ya que no existen dos patrones iguales, incluso en el caso de hermanos gemelos idénticos, es estable a lo largo de la vida de una persona e independiente de factores genéticos, por lo que es una de las técnicas biométricas idónea para entornos de alta seguridad.

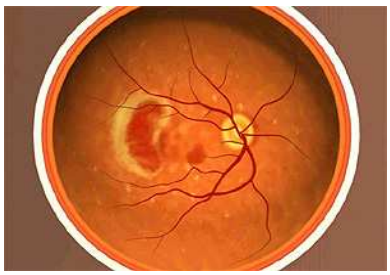


Figura 3.16 Vasos sanguíneos de la retina.

III.2.2.2.1. Captura y Proceso de la Imagen de la Retina.

De entre las ventajas de esta técnica se puede resaltar que es una de las técnicas biométricas más precisas, utiliza un rasgo fisiológico estable (la retina) y consigue tasas de falsa aceptación prácticamente nulas. Por el contrario, de entre sus importantes limitaciones destacamos que es una técnica intrusiva pues es necesario que el usuario se coloque muy cerca del dispositivo de captura, lo que provoca un importante rechazo. Por otra parte, existe una serie de enfermedades degenerativas de la retina, como las cataratas y el glaucoma, que pueden alterar la imagen de la misma a lo largo del tiempo. Estas limitaciones hacen que el desarrollo de este tipo de tecnología no sea tan rápido ya que existen otras técnicas biométricas que pueden proporcionar todas sus prestaciones con bastantes menos limitaciones.

No obstante, aunque esta tecnología no está actualmente muy desarrollada, es posible encontrar sistemas de muy reciente creación, como es el planteado por G. Heacock, D. Usher y J. Marshall, comercializado por la compañía *Retinal Technologies Inc*[4].

El proceso de adquisición de la imagen de la retina es el paso más difícil en cualquier sistema de identificación basado en la misma, pues es un órgano interno, pequeño y difícil de medir si se carece de un dispositivo apropiado especialmente diseñado para esta aplicación. Como ya se mencionó, el usuario debe situarse muy cerca del dispositivo de captura pues ya que la imagen se captura a través de la pupila y debe permanecer inmóvil durante la captura de la imagen ya que cualquier pequeño movimiento invalidaría el proceso de adquisición de la imagen y se tendría que empezar de nuevo.

Una vez realizada la captura de la imagen, se procede a obtener el patrón de retina mediante la extracción de las características de la red de vasos sanguíneos de la misma. En el sistema comercializado por Retinal Technologies Inc, el patrón de retina se obtiene después de realizar los siguientes pasos:

a) Extracción de los perfiles de intensidad de los vasos sanguíneos que cubren la retina.
b) Determinación del área de estudio.
c) Localización de los vasos sanguíneos
d) Generación del patrón de retina.

En la mayoría de los sistemas comercializados el tamaño del patrón de retina oscila entre los 50 y los 96 bytes. Por otra parte en este tipo de técnica biométrica, a juicio de sus desarrolladores, el proceso de comparación suele ser robusto.

III.2.3. Reconocimiento de la Geometría de la mano.

El uso de la geometría de diversas partes del cuerpo para identificar a las personas se inició en la época de los antiguos egipcios. En el siglo XIX, alrededor de 1870 el antropólogo francés Alphonse Bertillon propuso un sistema de identificación de personas basado en el registro de las medidas de diversas partes del cuerpo. Este método conocido como *Sistema Bertillon* o *Bertillonaje* fue adoptado por las policías de Francia y otras partes del mundo. En 1903 el sistema colapsa al ser sentenciado un hombre inocente en la penitenciaria norteamericana de Leavenworth, Kansas que tenía el mismo conjunto de medidas del hombre que había cometido el crimen. Desde el abandono de dicho sistema no se ha avanzado mucho en esta técnica biométrica.

La Real Academia Española define a la mano como una parte del cuerpo humano unida a la extremidad del antebrazo y que comprende desde la muñeca hasta la punta de los dedos. Anatómicamente la mano consta de un esqueleto óseo provisto de veintisiete

[4] http://www.retinaltech.com

huesos articulados entre sí, tiene los movimientos de pronación (palma hacia abajo), supinación (palma hacia arriba), extensión y flexión. Ésta última da a la mano la posibilidad de tomar objetos, que es la base de la actividad manual propia del humano y presenta además la posibilidad de oposición del dedo pulgar a los otros dedos que le permiten realizar trabajos de precisión.

En la mano existen fundamentalmente tres grupos de huesos (véase figura 3.17): los del *carpo, metacarpo* y *dedos*. El carpo es la parte más próxima de la mano, cercana a la muñeca, y consta de ocho huesos dispuestos en dos filas, cuatro en cada una. El segundo grupo está formado por los cinco metacarpianos y forman la parte más distal del esqueleto de la palma. El tercer grupo, los dedos, está constituido por los huesos de los dedos, las falanges, pequeñas y cortas, de las que hay tres en cada dedo, exceptuando el pulgar que tiene dos.

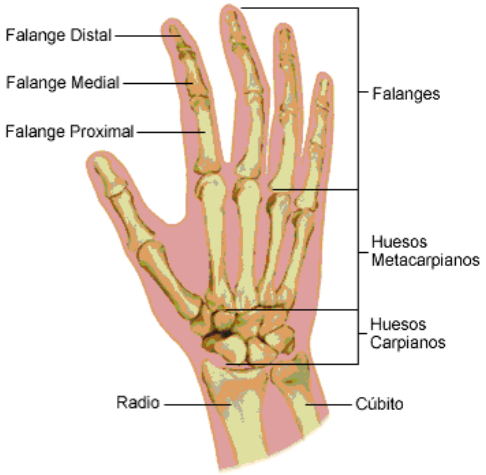


Figura 3.17 Huesos fundamentales de la mano.

Los músculos de la mano se dividen fundamentalmente en dos grupos: *flexores*, los de la *cara palmar*, y *extensores*, los de la *dorsal*. Existen también los músculos propios de la mano, dispuestos en tres regiones: *eminencia tenar*, *o del pulgar, eminencia hipotenar,* o del *bordel cubital,* y *región palmar* o media de la mano. En conjunto, los músculos de la mano son: cuatro de la eminencia tenar (flexor corto del pulgar, oponente del pulgar, abductor del pulgar, abductor corto del pulgar), cuatro de la eminencia hipotenar y once de la palma, cuatro lumbricales, cuatro interóseos dorsales y tres interóseos ventrales. En total, diecinueve músculos propios, más otros quince músculos del antebrazo.

Fisiológicamente la mano está dotada de la posibilidad de realizar una gran cantidad de movimientos gracias a la riquísima disposición muscular y del esqueleto óseo. Como ya se mencionó, la posibilidad de oposición del pulgar es una de las principales características de la mano del hombre.

El primer sistema comercial para reconocimiento de geometría de mano estuvo disponible a principios de los años 70. La Universidad de Georgia fue una de las primeras

instituciones en utilizarlo en 1974. El ejército de Estados Unidos lo probó para su uso en bancos en 1984, pero el concepto no fue patentado hasta 1985.
David Sidlauskas desarrolló y patentó el concepto de geometría de la mano en 1985 creando al mismo tiempo la empresa *Recognition Systems Inc.,* cuyo primer sistema comercial estuvo disponible al año siguiente. En los Juegos Olímpicos de 1996 se hizo uso de este tipo de sistemas para controlar y proteger el acceso físico a la Villa Olímpica.

III.2.3.1. Método de captura.

Para obtener los datos biométricos necesarios en este tipo de tecnología se hace uso de una cámara digital de baja resolución. La mano se coloca con la palma hacia abajo sobre una superficie plana que tiene 5 clavijas, que ayudan a alinear los dedos de la mano para asegurar una lectura exacta. La cámara captura entonces la imagen de la palma de la mano y su sombra. En la parte izquierda de la superficie plana, se coloca un espejo formando un ángulo de 60 grados; este espejo refleja hacia la cámara el perfil lateral de la mano (véase figura 3.18)

Figura 3.18 Vista frontal y lateral de la mano posicionada.

III.2.3.2. Preprocesado de la Imagen.

Una vez capturada una foto de la mano se inicia el bloque de preprocesado, en que se van a extraer los bordes de la imagen para su posterior entrada en el bloque de extracción de características.
El preprocesado empieza traduciendo la imagen de color a una imagen en blanco y negro con alto contraste entre la mano y el fondo. Para conseguir este resultado se opera con las distintas componentes de color de la imagen y aprovechando que la piel posee una débil componente de azul. La operación realizada es:

$$I_{ByN} = h(h(I_R + I_V) - I_A)$$

Donde I_{BYN}, I_R, I_V e I_A son, respectivamente, la imagen en blanco y negro resultante y las componentes roja, azul y verde de la imagen original. La función *h* representa la función de estiramiento del histograma. Esta operación intenta eliminar aquellas zonas de la imagen con mayor componente azul que roja y verde, ya que la diferencia dará negativa (en la operación de estiramiento re realiza una eliminación de los valores negativos, igualándolos a 0). Con esta operación todo el fondo pasará a ser negro (valor 0) mientras que la mano, al tener una componente azul muy inferior a las otras dos componentes, pasará a tener valores cercanos al 1 (cercano al blanco).

Tras realizar el paso a blanco y negro, la imagen se pasa a valores binarios utilizando un umbral. Este umbral ha sido seleccionado heurísticamente para que se eliminen valores no necesarios dados por brillos o ruidos en la imagen. A la imagen resultante se le puede aplicar un algoritmo de extracción de bordes basado en el operador de Sobel[5]. Con esta última operación se obtiene una imagen binaria que representa el borde de la imagen y, por lo tanto, el contorno del dorso de la mano y el de su perfil.

III.2.3.3. Extracción de Características.

Una vez obtenidos los contornos del dorso y del perfil de la mano, se realizan una serie de medidas que darán como resultado el vector de características correspondiente. Estas medidas se pueden dividir en cuatro tipos principales:

a) **Anchuras** de cada uno de los dedos salvo el pulgar (w11, w12, w13 y w14, para el dedo índice; w21, w22, w23, w24 y w25, para el dedo medio w31, w32 y w33, para el dedo anular w34 y para el dedo meñique w41, w42, w43 y w44). También se mide la anchura de la palma de la mano (w0) y las distancias entre los tres puntos inter –dedo P1, P2 Y p3 , en coordenadas tanto horizontales como verticales (P1x-P2x, P1x-P3x, P1x-P2y, P1x-P3y, donde los superíndices indican la coordenada tomada).

b) **Alturas** del dedo medio (h3), del dedo meñique (h2) y de la palma de la mano (h1).

c) **Ángulos** entre la línea de unión de los puntos inter-dedo y la horizontal: a_2, para el ángulo entre P_1-P_2 y la horizontal; a_3, para el ángulo entre P_1-P_3 y la horizontal.

d) **Desviaciones** de los dedos con respecto a la línea recta ideal que deberían formar las falanges. Estas distancias se miden como la distancia del punto medio del contorno del dedo (por ejemplo P12 para el caso del dedo índice) y el punto medio de la recta definida entre el punto inter-dedo correspondiente (P1 en el mismo

[5] El operador Sobel es utilizado en procesamiento de imágenes, especialmente en algoritmos de detección de bordes. Cuando es aplicado sobre una imagen digital en escala de grises, calcula el gradiente de la intensidad de brillo de cada punto (pixel) dando la dirección del mayor incremento posible (de negro a blanco) ; además calcula el monto de cambio en esa dirección, es decir, devuelve un vector. El resultado muestra qué tan abruptamente o suavemente cambia una imagen en cada punto analizado, y a su vez que tanto un punto determinado representa un borde en la imagen y también la orientación a la que tiende ese borde.

caso) y el punto más alto del contorno de ese dedo, en el que se hacen medidas (P14). De forma matemática para el dedo índice sería:

Donde los subíndices indican el punto medio y los superíndices la coordenada utilizada. De esta forma se obtiene *desv1, desv2, desv3* y *desv4* para los dedos índice, medio, anular y meñique respectivamente.

En la figura 3.19 se pueden observar las principales medidas tomadas.

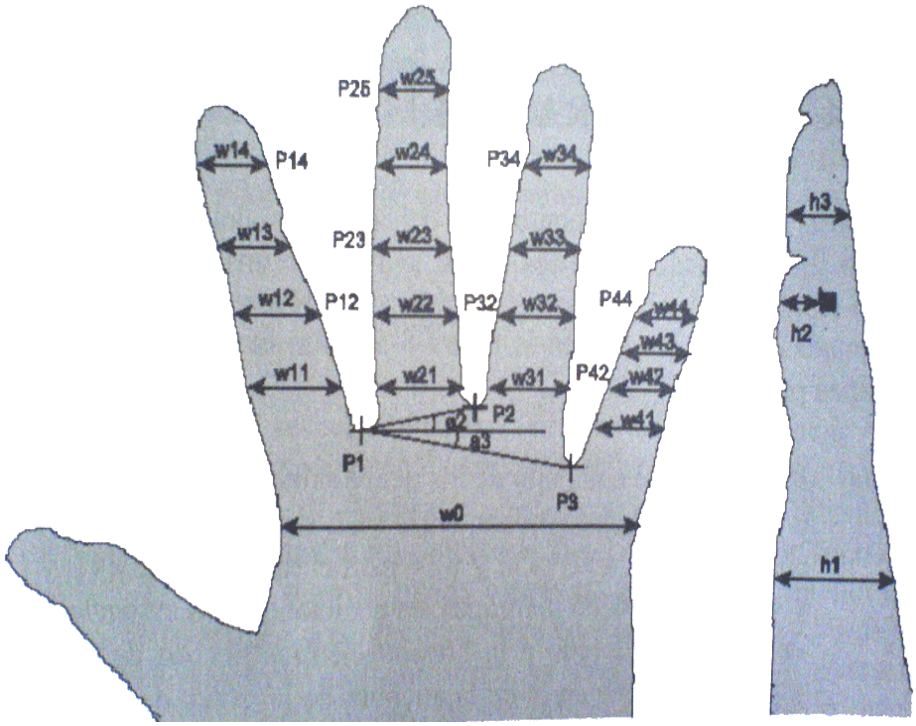


Figura 3.19 Esquema de las principales medidas tomadas.

Después de extraer las características necesarias, se lleva a cabo el proceso de inscripción, en el módulo de inscripción, que para un sistema de geometría de la mano requiere de la captura de tres o cuatro imágenes de la mano, debido a que un número mayor implicaría una gran molestia al usuario y un número menor sería insuficiente para poder crear un patrón con garantías.

Este tipo de tecnología biométrica cuenta con un estándar Internacional, creado por la ANSI, que es el ANSI INCITS 396-2005 Hand Geometry Interchange Format, que define el formato de intercambio de información para almacenamiento y transmisión de la información recolectada de la silueta de la mano. Define el contenido y el formato de la información así como las unidades usadas para hacer la medición de las características de la geometría de la mano. Sin embargo, este estándar aún no ha sido aprobado como un estándar oficial.

III.2.4. Reconocimiento de firma escrita.

La escritura es un sistema de representación gráfica de una lengua, por medio de signos grabados o dibujados sobre un soporte. Es un método de comunicación humana que se realiza por medio de signos visuales que constituyen un sistema y ha estado presente en todas las culturas que han existido a lo largo de la historia. La escritura actúa no solamente como pilar de la civilización, sino que también hace duraderos los logros de la misma. Pese a que la puesta en escena de nuevas tecnologías en almacenamiento y transmisión puede hacer pensar que la escritura pasa a segundo plano en la actualidad, el texto manuscrito sigue siendo la forma más natural y directa de registro de información. La continua automatización de los sistemas de administración de la Información ha favorecido la creación de tecnologías que permiten que sistemas automáticos realicen funciones que antiguamente llevaban a cabo personas. Sin embargo, todavía hay campos donde se requiere la presencia de un operario humano que supervise la tarea, como es el caso del procesado de cheques bancarios, clasificación y difusión de correos de los sistemas postales.
Por otra parte, la aparición de equipos informáticos sofisticados que permiten el uso de lápices y punteros con interfaz de usuario (PDA's, teléfonos móviles con pantallas táctiles, Tablet PC's, entre otros) ha reavivado el interés en el estudio de la escritura con objeto de su reconocimiento automático.

III.2.4.1. Adquisición de la firma escrita.

Las técnicas de adquisición de firma escrita se clasifican en dos grandes grupos: Técnicas off-line y técnicas on-line. En multitud de ocasiones en las que hay que efectuar el reconocimiento de firma sólo se dispone de éstas realizadas sobre papel. A la adquisición de este tipo de firma se le denomina captura off-line, debido a que la ejecución de dicha firma no coincide temporalmente con la adquisición de los datos. En este caso la firma se realizó en un momento indeterminado y posteriormente se efectuó la captura. Puesto que la información resultante de la ejecución de la firma es la imagen impresa en papel, la captura de la imagen consiste en la digitalización de dicha imagen.
Por otro lado y mediante el empleo de dispositivos tales como tabletas digitalizadoras o acelerómetros acoplados a bolígrafos, se puede realizar un muestreo temporal de la trayectoria del bolígrafo durante la ejecución de la firma. En este caso, el proceso de adquisición de los datos es simultáneo a la ejecución de la firma y se dice que la adquisición de los datos es on-line.

La principal diferencia entre los sistemas de adquisición on-line y off-line es la simultaneidad entre la realización de la firma y la adquisición de información de la misma. Como ya se mencionó la adquisición off-line consiste en la digitalización de la imagen de la firma. En este caso se pierde la información temporal, no se conoce su duración ni la secuencia ordenada de los trazos. Hay información de la dinámica y de la presión de la firma que se puede recuperar mediante el análisis minucioso de la dispersión de la tinta

en el papel, aunque debido a la dificultad de extraer esta información de forma automática, se considera perdida. Esto hace que la información que se utilice normalmente en sistemas off-line se limite a información estática.
En cambio, mediante la adquisición on-line no sólo se dispone de la información geométrica, sino también de la información dinámica y temporal de la firma: duración, secuencia ordenada de ejecución de los trazos, velocidades y aceleraciones de la mano, entre otras. Además dependiendo de las especificaciones del dispositivo empleado en la captura on-line, también se puede obtener información adicional como la presión instantánea ejercida a lo largo de la firma, o los ángulos de inclinación del bolígrafo.

III.2.4.2. Acondicionamiento de la señal de la firma.

La etapa de acondicionamiento de la señal de la firma tiene básicamente tres objetivos:

- Eliminar la información que no sea relevante para el reconocimiento.
- Corregir la información degradada durante la adquisición.
- Reducir la variabilidad entre distintas realizaciones de una misma firma.

La forma de implementar este preprocesado depende de la naturaleza de los datos disponibles y, por lo tanto, del tipo de adquisición efectuada. Esto lleva a diferenciar el preprocesado de firmas off-line y on-line.

Φ **Acondicionamiento para la firma off-line.**
Puesto que la adquisición off-line consiste en la digitalización de la imagen de la firma, las técnicas que se emplean en el preprocesado de la información son básicamente técnicas de procesado digital de la imagen, por lo cual se llevan a cabo las siguientes etapas:

a) Binarización: Se puede realizar estableciendo un umbral fijo a priori o mediante algoritmos de cálculo automático del umbral a partir del histograma de niveles de gris de la imagen.
b) Eliminación de Ruido: Se puede realizar antes (mediante filtros pasa baja) o después del proceso de binarización (mediante la unión de trazos cortados o llenando huecos).
c) Segmentación: Consiste en aislar los trazos que contienen la información necesaria para caracterizar una firma. Se puede extraer toda la firma o solamente el cuerpo de la misma, eliminando los trazos estadísticos exteriores.
d) Normalización en Posición y Tamaño: Dependiendo del algoritmo de clasificación que se utilice a continuación, puede ser necesaria la normalización en posición (respecto al punto inicial) y en tamaño.
e) División de Celdas: Consiste en la división de la imagen en celdas de manera que cada una de ellas tenga una percepción local de la firma. La extracción de parámetros se aplica entonces a cada celda.

Φ **Acondicionamiento para la firma on-line.**

En el preprocesado de firmas capturadas on-line se busca obtener una representación robusta respecto a las tres variaciones geométricas básicas: rotación, traslación y escalado de las diferentes realizaciones de las firmas. Algunos ejemplos de preprocesado aplicados a la firma on-line son los siguientes:

a) Alineamiento Respecto a la Posición: Algunos ejemplos de referencias comunes son el punto inicial o el centro de masas.
b) Normalización en rotación: Hay diversas opciones, como alinear respecto al ángulo de la trayectoria media, obtener una representación de la firma en coordenadas polares y normalizar respecto al ángulo medio, o normalizar respecto al eje de mínimo momento de inercia.
c) Normalización del Tamaño: Se suele normalizar respecto a valores extremos de las coordenadas, rangos de variación o estadísticos de primer y segundo orden.

III.2.4.3. Extracción de Características y Representación de la firma.

Una vez capturada la información de la firma, es conveniente generar o seleccionar aquellas características que faciliten el reconocimiento. Para que las características elegidas representen de forma óptima a la firma deben cumplir dos requisitos:

- Deben ser discriminantes entre firmas verdaderas y falsificaciones.
- Deben permanecer estables ante las variaciones típicas de las firmas verdaderas.

De forma simplificada, una característica será buena cuando, para diferentes realizaciones de un mismo usuario, su varianza sea pequeña y su valor medio esté bien separado del valor medio obtenido para firmas falsas.

De igual forma las características extraídas de la firma se pueden clasificar atendiendo a varios criterios. Dos posibilidades son:

- En función de su naturaleza. En este caso podemos encontrar características dinámicas y estáticas. Las características dinámicas toman información temporal del proceso de realización de la firma (velocidades, posiciones, duraciones parciales o totales de levantamientos de trazos). Las características estáticas toman información geométrica de la firma (inclinación de los trazos verticales, localización de inicios y finales de trazos).
- En función del ámbito de representación. En este caso se distingue entre características globales y locales. Las características globales toman información de la firma en su totalidad como una unidad. Algunas características globales son: duración total, medias y desviaciones típicas y centro geométrico. Las

características locales son aquellas que toman información de puntos o zonas específicas de la firma, ya sea en el dominio temporal o en el espacial. Entre las características locales típicas se pueden encontrar: valores instantáneos de los diferentes parámetros y puntos máximos y mínimos.

La fase de extracción de características va a influir en la forma final de estructurar el modelo o patrón de la firma. A continuación se introducen los dos tipos básicos de representación de firmas empleados en los diferentes sistemas de reconocimiento.

Φ **Representación paramétrica.** En este caso las características consisten en un conjunto de parámetros o valores individuales calculados a partir de la información adquirida y procesada. Sus valores suelen agrupar en un vector que representa la firma. Algunos parámetros típicos que podemos encontrar son: velocidad de escritura máxima, mínima y media, velocidades de escritura en los diferentes ejes, duraciones globales y locales, entre otras.

Φ **Representación mediante funciones.** Otra forma de representar la firma es como una función temporal o espacial que refleja la evolución de ciertos parámetros a lo largo de la realización de la firma. Las representaciones temporales solamente se pueden aplicar sobre firmas adquiridas de forma on-line y consisten en el muestreo de los parámetros adquiridos mediante el dispositivo a una cierta frecuencia de muestreo y la extracción, a partir de éstos, parámetros adicionales. Algunas funciones temporales son: posición, presión, fuerza, entre otros.

Es un hecho que ningún sistema de identificación personal está libre de error. Sin embargo, dependiendo de la tecnología y de las condiciones de los datos tomados, este error puede ser aceptable para determinadas aplicaciones. En concreto, las tasas de error en los sistemas de reconocimiento de firma escrita dependen fundamentalmente del tipo de falsificaciones que se consideren. Existen dos tipos de falsificaciones: falsificaciones reales y falsificaciones casuales. Se habla de falsificaciones reales cuando el impostor conoce la firma original y ha podido entrenarse en la realización de la falsificación. Cuando las falsificaciones son casuales, se hace referencia a que se han empleado las firmas originales de otros usuarios para llevar a cabo la falsificación. Como es de esperar, las tasas de error al considerar falsificaciones reales son superiores cuando se considerar falsificaciones casuales.

III.2.5. Reconocimiento de Voz.

La comunicación mediante el habla es la forma más habitual de transmitir información entre personas. En este tipo de comunicación, la identidad del interlocutor va a estar fuertemente correlacionada con las características fisiológicas y de comportamiento del mismo (hábitos lingüísticos, entonación de las frases, entre otras). Las bases para el reconocimiento de voz fueron desarrolladas por la compañía Texas Instruments alrededor de 1960 y desde ese momento la identificación por voz ha estado bajo intensas

investigaciones y desarrollos. A pesar de esto, la variabilidad presente en la señal de la voz al momento de llevar a cabo el proceso de identificación haciendo uso de sistemas reconocedores de voz resulta perjudicial pues el locutor no puede repetir de forma exacta una misma frase o palabra.

III.2.5.1. Principios de Funcionamiento de los Sistemas de Reconocimiento de Voz.

Este tipo de Sistemas deben ser capaces de trabajar de tres formas distintas:

a) Modo de Entrenamiento: En esta fase se obtienen los patrones y valores de referencia correspondientes a cada uno de los usuarios.
b) Modo de Funcionamiento o servicio: Esta es la fase de utilización del sistema, y en la cual a partir de señales de voz el sistema tomará decisiones acerca de la identidad del locutor.
c) Modo de actualización: Durante la vida útil del sistema, éste deberá ser capaz de incorporar nuevos locutores, dar de baja a usuarios, y opcionalmente actualizar o mejorar modelos y referencias correspondientes a los usuarios presentes del sistema.

En la figura 3.20 podemos observar el diagrama de bloques de un sistema de reconocimiento de voz. Como se puede observar el sistema parte de una realización acústica (una palabra o sucesión de palabras) procedente de un locutor no identificado. En primer lugar será tarea del sistema la conversión de la señal acústica en una serie de vectores de características que extraigan de forma eficiente la información presente en la señal de voz. Esta función será realizada en el módulo de preprocesado acústico.

El sistema debe disponer de patrones correspondientes a los distintos locutores "conocidos" por el sistema. Estos patrones habrán sido obtenidos en la fase de entrenamiento del sistema a partir de la señal de voz procedente de cada uno de los locutores que se va a incorporar al sistema, y serán almacenados en el módulo de patrones y referencias.

Una vez obtenidos los vectores de características correspondientes a la señal de voz de entrada, y teniendo disponibles los patrones correspondientes a los distintos locutores, el sistema debe disponer de un método para obtener el parecido o similitud entre la realización acústica de entrada y cualquiera de los modelos conocidos por el reconocedor. Este proceso será realizado en el módulo de cálculo de similitudes.

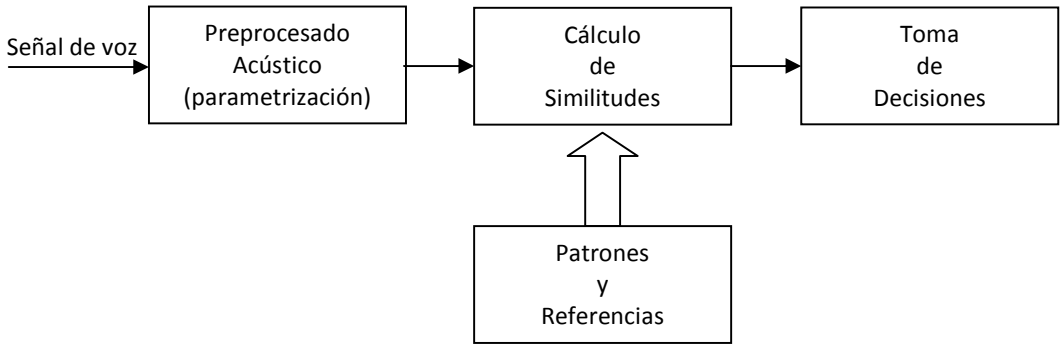


Figura 3.20 Diagrama de bloques de un sistema de reconocimiento de locutores.

Por último, a partir de los valores de similitud obtenidos, el sistema deberá tomar una decisión acerca de la identidad del locutor que ha generado la señal de voz de entrada. Es precisamente este módulo de Toma de Decisiones el que mayor atención debe recibir por parte del diseñador del sistema, ya que es la única salida observable por el usuario y por el proveedor del servicio.

III.2.5.2. Clasificación de Sistemas de Reconocimiento de voz.

La primera gran diferencia entre sistemas viene dada por la dependencia del sistema al texto o mensaje que se necesita pronunciar, teniendo de esta forma lo que llamaremos sistemas dependientes de texto, basados en palabras o frases claves; o sistemas independientes de texto, donde no habrá restricción en el contenido lingüístico del mensaje.
La segunda gran clasificación que podemos hacer, y que va a influir de forma significativa en la estructura del sistema final, es entre sistemas de identificación o verificación de locutores. El objetivo de los *sistemas de identificación de locutores* es clasificar una señal de voz, cuyo origen es desconocido, como perteneciente a uno de entre un conjunto de n locutores. Dentro de estos sistemas, debemos diferenciar dos posibles casos:

i. Identificación en conjunto cerrado: En este caso, el resultado del proceso es una asignación de identidad a uno de los locutores modelados por el sistema, y conocidos como usuarios.
ii. Identificación en conjunto abierto: Aquí se debe considerar una posibilidad adicional a las del caso anterior, y es la posibilidad de que el locutor que pretende ser identificado no pertenezca al grupo de usuarios, con lo que debería ser catalogado como *impostor* al intentar ser identificado como usuario del sistema.

Por el contrario, los *sistemas de verificación de locutores* toman dos entradas: una de ellas es la señal de voz a verificar, y la otra es una solicitud de identidad, que puede ser

realizada de diversas formas: lectura de tarjeta magnética individual, mediante el tecleado de un código de locutor, entre otras. De este modo, las dos únicas salidas o decisiones del sistema son la aceptación o el rechazo del locutor.

III.2.5.3. Aplicaciones Actuales y Líneas Futuras de Trabajo.

La tecnología de reconocimiento de voz está lista para su uso en diversas aplicaciones, en las que dependiendo del grado de libertad que posean tanto el locutor como el sistema en sí obtendrán rangos de rendimientos diferentes. El uso más común de las tecnologías de reconocimiento de voz es en el control por comandos; los sistemas se utilizan para dar órdenes a una computadora, por ejemplo para abrir o cerrar aplicaciones. Otra aplicación de este tipo de tecnología son los sistemas diseñados para personas con capacidades diferentes; en concreto para personas con problemas auditivos o que tienen dificultad para introducir información a una computadora a través del teclado, pues permiten obtener texto escrito a partir del habla.
La identificación mediante el reconocimiento de voz se está introduciendo muy lentamente al mercado, una de las principales razones es que este tipo de tecnología presenta altos índices de error; los sistemas tienden a tener muchos falsos rechazos debido principalmente a ruidos de fondo.

Con el objetivo de propiciar el avance de las tecnologías de reconocimiento de voz, existen diferentes líneas de actividad en las que los grupos de investigación más importantes del mundo exponen y desarrollan sus investigaciones. Como puntos de referencia a nivel mundial es imprescindible mencionar congresos como Odyssey[6] y las evaluaciones anuales llevadas a cabo por NIST[7]. En dichas evaluaciones se comparan los rendimientos de sistemas de reconocimiento de voz pertenecientes a diferentes grupos de investigación.

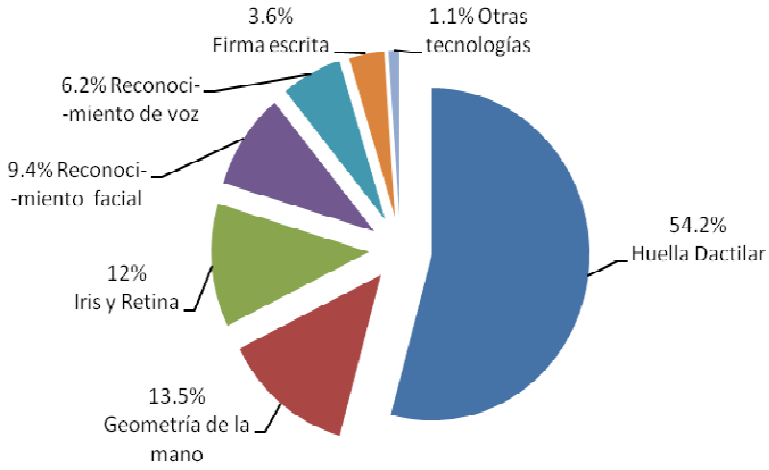
III.3. Por su uso.

Según información proporcionada por el International Biometric Group[8], las tecnologías biométricas más utilizadas durante el año 2007 fueron las siguientes: el reconocimiento de huellas dactilares (con un 54.2%), la geometría de la mano (con un 13.5%), el escaneo de Iris y retina (con un 12%), el reconocimiento facial (con un 9.4%), el reconocimiento de voz (con un 6.2%), el análisis de firma escrita (con un 3.6%) y otras tecnologías (con un 1.1%). Una distribución detallada de estos porcentajes se puede observar en la gráfica 3.1.

[6] www.odyssey04.org

[7] www.nist.gov/speach

[8] http://www.biometricgroup.com/



Gráfica 3.1 Porcentaje de tecnologías biométricas más utilizadas.

CAPÍTULO IV

Estándares Biométricos

IV.1. Definición de Estándar.

Un estándar es un conjunto de reglas que deben cumplir los productos, procedimientos o investigaciones que afirmen ser compatibles con el mismo producto. Los estándares ofrecen muchos beneficios, reduciendo las diferencias entre los productos y generando un ambiente de estabilidad, madurez y calidad en beneficio de consumidores e inversores.

La carencia de estándares biométricos a nivel industrial ha dificultado el desarrollo de algunos tipos de sistemas biométricos y el crecimiento de este sector industrial. Sin embargo, la industria biométrica está teniendo un papel muy activo para solucionar el problema de la carencia de estándares generando resultados que empiezan a ser ampliamente aceptados por los industriales y marcando el camino a seguir en un futuro próximo. Los esfuerzos que se están realizando y los ya realizados han perseguido distintos objetivos que van desde la definición de API (Interface de Programación de Aplicaciones), los formatos de los ficheros con la información de parámetros biométricos, la encriptación de la información biométrica, la interacción entre dispositivos biométricos diferentes, etc.

IV.2. Papel de los estándares biométricos.

Actualmente, la mayoría del hardware y software relacionado con los distintos sistemas biométricos están basados en tecnología propietaria (no estándar) de las empresas que los fabrican. Son varios los aspectos en los que estos dispositivos varían, por ejemplo la forma en que los sensores biométricos y los sistemas con las aplicaciones se comunican, el método utilizado para extraer las características con información discriminante de las muestras biométricas (huellas digitales, voz, imagen del iris, etc) que se toman y procesan en cada caso, las técnicas o métodos de comparación de los patrones, la longitud y el contenido de los patrones, incluidos el método de almacenamiento y recuperación de los datos biométricos.

Como consecuencia de esto, cuando una compañía se decide por una determinada tecnología biométrica para integrar en alguno de sus productos o para producirla ella misma, queda “atada” a la misma en el futuro pues si en algún momento, decidiese incorporar nueva tecnología de esta naturaleza tendría que volver a implementar su sistema o al menos gran parte del mismo. Debido a la naturaleza emergente de esta tecnología y a la poca madurez de muchos productos de biometría, los desarrolladores de aplicaciones que hacen uso de tecnología biométrica temen que las empresas fabricantes de dicha tecnología cambien de rumbo o modifiquen sus productos obligándoles a “tirar” gran parte del trabajo que hayan realizado así como su dinero.

Sin embargo, se debe aclarar que el desarrollo de estándares biométricos y su adopción general, no asegurará una total compatibilidad entre dispositivos y tecnologías y que, en muchos casos, seguirá siendo necesaria una adaptación de los antiguos sistemas o

aplicaciones para que funcionen con los nuevos dispositivos o tecnología que se decida utilizar. Esto es debido a que los algoritmos y los procesos diseñados e implementados por los fabricantes de tecnología biométrica para la extracción de los datos o muestras, el proceso de extracción de las características de las mismas, e incluso el proceso de autenticación biométrica del usuario difícilmente llegarán a ser estándares de la industria al constituir el "valor añadido" tecnológico de las mismas. Sin embargo, es de esperar que el desarrollo y la utilización de los estándares biométricos permita a los desarrolladores-integradores de aplicaciones con tecnología biométrica puedan optar por un amplio rango de dispositivos y tecnologías intercambiables de una forma directa, es decir, sin necesidad de las ya mencionadas adaptaciones, de ese modo los riesgos que se mencionaron se verán reducidos de forma significativa.

IV.3. Estándares Biométricos Internacionales.

IV.3.1. BioAPI.

El consorcio BioAPI nace en Abril de 1998 durante la conferencia CardTech/SecureTech con el apoyo de algunas de las compañías informáticas más importantes a nivel internacional como IBM y Hewlett-Packard. La primera especificación apareció en Septiembre de 2000 y la especificación final en Marzo de 2001. La idea era desarrollar una alternativa a otras iniciativas de estandarización. BioAPI ha llegado a ser uno de los esfuerzos más relevantes en la generación de estándares biométricos con varios objetivos como: desarrollar una Interfaz de Programación de Aplicaciones (API por sus siglas en inglés) independiente del parámetro biométrico y del hardware de los distintos fabricantes, crear un estándar independiente del sistema operativo, trabajar de forma coordinada con desarrolladores e integradores de aplicaciones con elementos biométricos para generar una API de fácil uso y de fácil convivencia con otros estándares ya existentes, entre otros.

Desde un punto de vista general, BioAPI intenta estandarizar el modo en el que las aplicaciones se comunican con los dispositivos biométricos y la forma en la que los datos son almacenados y utilizados, ofreciendo a los desarrolladores un conjunto común de llamadas a funciones para interactuar modularmente con los distintos dispositivos biométricos, algoritmos, etc. Sin embargo, no pretende estandarizar el modo en el que los datos son generados por los dispositivos biométricos, ni entrometerse en los rasgos distintivos que define la tecnología biométrica de cada fabricante. El resultado de ello es que, en algunos casos, obliga a los usuarios a 're-entrenarse' en el uso de estos dispositivos.

Las funciones de BioAPI cubren aspectos como el entrenamiento, la verificación e identificación de usuarios, la captura de datos, el proceso de los mismos, la comparación de patrones y el almacenamiento de la información biométrica. Establece un alto nivel de abstracción que permite a los desarrolladores olvidarse de los detalles particulares de

fabricación de los distintos productos y de las tecnologías empleadas por los diferentes fabricantes.

Actualmente muy pocas soluciones en esta área son compatibles con BioAPI aunque es muy importante resaltar que es un estándar ampliamente aceptado por la industria biométrica, incluso es apoyado por agencias estatales como es el caso de Estados Unidos. Esta participación y apoyo por parte de tantos interlocutores ha prolongado el tiempo de desarrollo de este estándar, que tardó varios años en producir su versión 1.0. Esto puede convertirse en un problema a medio plazo ya que otros estándares están apareciendo con un mayor dinamismo y con un gran empuje, apoyados por otros grandes fabricantes de tecnología como es el caso de BAPI y Microsoft.

IV.3.2. Estándar BAPI.

BAPI es un nuevo estándar biométrico desarrollado y planeado por un vendedor de soluciones biométricas llamado I/O Software en lugar de un consorcio de compañías e instituciones como fue el caso de BioAPI. En Mayo de 2000, Microsoft licenció BAPI, aunque había sido uno de los primeros en apostar por BioAPI, con la intención de incluirlo en las futuras versiones de sus sistemas operativos (Windows). BAPI se fusionó con su predecesor BioAPI llegando casi a reemplazarlo. La idea de que la tecnología biométrica forme parte de un sistema operativo ha hecho madurar esta área tecnológica, dejando de ser considerada como una tecnología del futuro y formado parte de un panorama actual de posibilidades a tener en cuenta a la hora de desarrollar aplicaciones. Arrastrados por la iniciativa de Microsoft, otras compañías como Intel han apostado por BAPI, licenciando este estándar para incluirlo en sus plataformas PC móviles y dotarlas de aspectos de seguridad.

En la actualidad el mundo de los estándares biométricos se encuentra dividido entre BAPI (apoyado por el consorcio Microsoft / Intel, en el que han colaborado otras compañías que también participan en el consorcio BioAPI) y BioAPI (considerado como el estándar de facto por agencias del gobierno de Estados Unidos para sus aplicaciones de seguridad). Esto nos conduce a una situación indeseada, contraria a la propia naturaleza de los esfuerzos encaminados a la generación de un único estándar. En los próximos años, BioAPI y BAPI deberán tener que ser considerados por todos los desarrolladores de aplicaciones hasta que ambos converjan en un único y definitivo estándar biométrico.

IV.3.3. CBEFF (Common Biometric Exchange File Format).

Se ha desarrollado un estándar conocido como Formato de Ficheros Común para el Intercambio Biométrico (CBEFF), cuyo objetivo es definir los formatos de los patrones biométricos para facilitar el acceso y el intercambio de diferentes tipos de datos biométricos a los sistemas que integran esta tecnología o entre diferentes componentes de un mismo sistema. CBEFF establece un formato para la cabecera de los ficheros

definiendo campos obligatorios y opcionales que proporcionan elementos comunes (opciones de seguridad, de integridad de los datos, fecha de creación del fichero, firma, tipo de parámetro biométrico, etc, para el intercambio de información entre los dispositivos biométricos y los sistemas que hacen uso de los mismos, además favorece la interoperatividad entre las aplicaciones biométricas y los sistemas, simplifica la integración del software y el hardware, y posibilita la compatibilidad futura frente a los nuevos avances tecnológicos que se vayan produciendo. CBEFF no busca soluciones de interacción con los dispositivos o con los procesos, sino un método común para manejar los datos biométricos.

La definición e implementación de este estándar está siendo considerada para su incorporación en dispositivos como las tarjetas inteligentes bajo los auspicios del grupo de trabajo NIST/BC Biometric Interoperability, Performance and Assurance Working Group.

Actualmente BioAPI y CBEFF se han unido para construir un frente común a la estandarización biométrica. Muchos fabricantes están adoptando este estándar ofreciendo soluciones compatibles CBEFF, lo que implica que los ficheros que contienen los datos de los patrones biométricos tienen esta cabecera común.

IV.3.4. Estándar ANSI X9.84.

La industria de servicios financieros tiene necesidades particulares en cuanto a la integración de soluciones biométricas en sus propios procesos y sistemas. Estas necesidades especiales influyen en la definición de los estándares biométricos recomendados por la industria financiera para la creación e integración de productos biométricos en sus plataformas y soluciones. Existe una organización acreditada por el Instituto Nacional de Estándares de Estados Unidos (American National Standars Institute, ANSI) conocida como X9 que es responsable del desarrollo y la publicación de los consensos alcanzados en temas de estandarización para la industria de servicios financieros. Entre las tareas encomendadas a esta organización podemos destacar la comprobación de procesos, la comprobación de las transacciones electrónicas comerciales y personales, la gestión y la protección de los códigos de autenticación personal (PIN), el uso de técnicas criptográficas, pagos a través de Internet, intercambio de imágenes financieras, aspectos de seguridad de la banca en línea, etc. Es fácil deducir que muchas de estas líneas de actividad despiertan el interés de empresas de soluciones biométricas que ofrecen el acceso lógico a esas aplicaciones o servicios mediante el empleo de información biométrica como si se tratase de claves públicas cuyo desciframiento no debería comprometer a los sistemas ni a los individuos. Por ello, dentro de X9, el grupo de trabajo X9.84-2000 (Biometric Information Managment and Security) se encarga de la estandarización biométrica, preocupados por la seguridad y la gestión de los datos biométricos de los usuarios durante el tiempo de su existencia. Aspectos como la seguridad en la transmisión y en el almacenamiento de esta información biométrica sensible, o la seguridad e integridad en el hardware y software utilizado, constituyen

algunos de sus objetivos. Su misión es desarrollar los estándares biométricos necesarios antes de empezar a realizar grandes inversiones en esta tecnología para incluirla en sus propios servicios. El estándar X9.84 se aprobó en Marzo de 2001 y se pretende que también se convierta en un estándar ISO.

X9.84 ha revisado el flujo seguido por los procesos de autenticación para detectar posibles riesgos de seguridad, puntos débiles en el mismo, etc. Su idea es que, si el sistema es consistente, los bancos e instituciones similares pueden implementar soluciones con la confianza suficiente en las fuentes de datos (bases de datos con los patrones biométricos), en los resultados de la verificación que se produzcan, en la integridad y confidencialidad de los datos que intervienen en el proceso de autenticación, en los procesos de transmisión y almacenamiento de esos datos, etc.

El estándar X9.84 proporciona integridad y privacidad. La privacidad se consigue mediante técnicas criptográficas aplicadas sobre los datos biométricos específicos del usuario, después de aplicar la técnica criptográfica estos datos se concentran en un bloque de datos, el cual se conoce como "opaco". La integridad se alcanza aplicando de igual manera técnicas criptográficas como las firmas digitales o un mensaje con un código de autenticación (Message Authentication Code, MAC) sobre todos los datos biométricos, es decir, la cabecera y el bloque de datos opaco con la información biométrica específica de ese usuario. La privacidad y la integridad pueden conseguirse de forma independiente, pero cuando se requieren ambas, primero se consigue la integridad, es decir, la firma y posteriormente la privacidad, es decir, se cifran las dos.
En particular X9.84 soporta el transporte de claves asimétricas, acuerdos entre claves, etc, tanto para la privacidad como para la integridad.

Aunque X9.84 se ha convertido en un estándar de facto para las compañías que ofrecen servicios financieros, no se puede decir lo mismo para los fabricantes o vendedores de soluciones biométricas especialmente los que se encargan de las funciones de almacenamiento, transmisión, extracción y comparación de los datos, ya que el nuevo estándar les obliga a incorporar un nivel de seguridad y mecanismos criptográficos que no se encuentran implementados en los productos actuales.

IV.4. Otras Iniciativas.

IV.4.1. NCITS-B10.8 (National Committee for Information Technology Standars).

Existe un comité acreditado por el Instituto Nacional de Estándares Americano (ANSI) conocido como NCITS (Comité Nacional para los Estándares en Tecnología de la Información) o X3, cuyo objetivo es generar estándares consensuados, de forma voluntaria, teniendo en cuenta el mercado, en las áreas de multimedia, intercomunicación

entre sistemas de información y computadoras, medios de almacenamiento, bases de datos, seguridad y lenguajes de programación. Toda la documentación que genera se conoce como ANSI NCITS, está formado por 35 comités, uno de los cuales se llama B10, que se dedica al desarrollo de estándares para las tarjetas de identificación y otros dispositivos relacionado ellas. Dentro de B10 un primer grupo de trabajo es B10.8 que se especializa en las licencias de los conductores y tarjetas de identificación similares. Una fuerza de trabajo dentro de B10.8 ha desarrollado un estándar biométrico de gran interés como es la definición de un método común para extraer y procesar las características conocidas como *minucias* de la imagen de una huella digitalizada. De esta forma la introducción de esta información biométrica en las licencias de los conductores, con el fin de verificar que las licencias pertenecen a quien las porta, está cada vez más cerca.

IV.4.2. CDSA / HRS (Common Data Security Architecture Specification / Human Recognition Services).

Es una arquitectura que se encuentra parcialmente involucrada en el desarrollo de estándares biométricos, fue creada por Intel en Diciembre de 1997 con la participación de Netscape, JP Morgan, Shell, IBM, Motorola y HP. El CDSA / HRS está desarrollando una herramienta de Software multiplataforma y segura para aplicaciones que incluyan elementos de comercio electrónico, comunicaciones y contenido digital. Trabajan directamente con el consorcio BioAPI con el fin de maximizar el consenso sobre la herramienta que está bajo desarrollo. El CDSA está desarrollando una API común a la que los programadores puedan añadir funcionalidad de autenticación. El componente HR es una extensión de la arquitectura propuesta por el CDSA relacionada directamente con el proceso de autenticación. La adopción de esta arquitectura puede ser una gran ayuda en el desarrollo de la industria biométrica, que vería a los distintos sistemas y tecnologías como parte de un todo.

IV.4.3. HA-API (Human Authentication Application Program Interface).

El Consosrcio Biométrico americano (US Biometric Consortium) dirige, de forma coordinada con el gobierno americano, los esfuerzos en biometría que se llevan a cabo en Estados Unidos desde 1993. Su principal logro ha sido el desarrollo de una Interfaz de Programación de Aplicaciones para la Autenticación de Personas (HA-API). La primera especificación de esta API se anunció a finales de 1997.

El proyecto se divide, esencialmente, en dos partes: la creación de una API biométrica genérica junto con la implementación de una prueba de concepto y la integración de la API en sistemas comerciales de autenticación que funcionan en red.

IV.4.4. NBCT (United States National Biometric Test Center).

Este centro fue creado por el Consorcio Biométrico del Departamento de Defensa Americano a finales de 1997. Su principal objetivo es llevar más lejos los esfuerzos en estandarización biométrica relacionados por el gobierno de los Estados Unidos, generando procedimientos estándares de prueba o validación y midiendo objetivamente el rendimiento de los sistemas biométricos implementados existentes en el mercado. Esa metodología permitirá comparar los sistemas biométricos entre sí, ofreciendo información sobre el avance real de la tecnología.

IV.4.5. INCITS M1 (Technical Committee for Biometrics).

Los atentados ocurridos el 11 de Septiembre de 2001 en los Estados Unidos, causaron una reacción en el gobierno americano respecto al camino que se estaba siguiendo en el desarrollo de la tecnología biométrica, con el fin de asegurar que el uso de esta información y tecnología fuese el adecuado. En Noviembre de 2001 el comité Técnico M1 del INCITS fue creado con el objetivo de establecer un foro para el desarrollo de estándares biométricos genéricos dentro de los Estados Unidos. Este comité ha retomado todos los esfuerzos llevados a cabo con anterioridad en esta área incluidos BioAPI, CBEFF y la estandarización de los formatos de los patrones biométricos.

Uno de los objetivos del Comité M1 es acelerar el empleo de los, cada vez mejores, sistemas de autenticación biométrica para entornos gubernamentales donde la seguridad de la nación, la defensa y la prevención de la usurpación de identidades falsas dentro y fuera del país. M1 actúa como el grupo consejero en la organización internacional ISO/IEC JCT 1/SC 37 en temas biométricos. Es responsable de establecer la posición del gobierno americano y de realizar contribuciones al SC 37 en todas las reuniones de este comité internacional. Además, M1 ha creado a su vez cuatro grupos de trabajo para poder controlar la creciente actividad en biometría de un modo racional y especializado:

M1.1: especializado en formatos de intercambio de datos biométricos (Biometric Data Interchange Formats).
M1.2: dedicado a las interfaces biométricas con un enfoque técnico (Biometric Technical Interfaces).
M1.3: trabaja en la interoperabilidad en los sistemas (Biometric Profiles).
M1.4: cuyo objetivo es la evaluación y la generación de informes en los sistemas biométricos (Biometric Performance Testing and Reporting).

IV.5. Organismos de Estandarización Nacionales.

IV.5.1. Asociación Mexicana de Biometría e Identidad (AMBI).

La AMBI fue creada en 2007 por el Ingeniero Mexicano Humberto López Gallegos con el objetivo de promover el uso de mejores prácticas que pudieran contribuir a lograr una mayor eficiencia y seguridad en el uso masivo de soluciones biométricas e identificación así como posicionar los desarrollos hechos en México en otros países, principalmente en Estados Unidos, en Europa y especialmente en Latinoamérica. Otro aspecto que el Ingeniero y actual presidente de la Asociación consideró crucial para su creación es el marco jurídico alrededor del uso de tecnología biométrica puesto que no existe nada escrito que regule en México el uso de los datos biométricos de las personas por lo que una de las iniciativas de la AMBI es la de participar activamente en la generación de estándares y normas de identificación para uso masivo de esta tecnología no solo en México sino en muchos otros países, convirtiendo a México en un modelo a seguir en esta disciplina.

La AMBI, cuenta con el apoyo de compañías como Bioscrypt, LG Iris, SAGEM, Digital Persona, Crossmatch, L1, Quometrics, HID, Kimaldi, Ingressio y Nitgen y tiene como misión la consolidación de la industria de tecnología biométrica e identificación conduciendo foros de discusión, coadyuvar como el brazo tecnológico de las principales asociaciones de verificación de identidad a nivel internacional, generar y divulgar masivamente contenidos relevantes al aprovechamiento de las tecnologías biométricas.

Entre los servicios que ofrece la AMBI se encuentran el Análisis de desempeño de Identificación, Certificación de Aplicaciones, Capacitación especializada a través de cursos básicos de biométrica con la posibilidad de tomarlos directamente con el fabricante de alguna tecnología biométrica, Asesorías especializadas para proyectos de Identificación, los cuales se pueden solicitar a la página de Internet de la Asociación[1], sin embargo, para que la solicitud de servicio sea procesada se deberá de ser miembro de la AMBI.

Por el momento, y a pesar de contar con el apoyo de las compañías ya mencionadas, la AMBI no ha desarrollado ningún estándar para el uso de tecnología biométrica en el país y tampoco ha participado en la creación y/o mejora de estándares internacionales. En la página de Internet de la Asociación no se da información acerca de cuál es el plan o estrategia que la AMBI está llevando a cabo o implementará en un futuro para participar en la creación de estándares de manera nacional e internacional.

[1] http://www.ambi.org.mx/

IV.5.2. Norma Oficial Mexicana.

Conforme a la Ley Federal sobre Metrología y Normalización, una Norma Oficial Mexicana es la regulación técnica de observancia obligatoria expedida por las dependencias competentes, conforme a las finalidades establecidas en el artículo 40, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como, aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado y las que se refieran a su cumplimiento o aplicación.

En materia de normalización esta ley tiene como objetivos:
♣ Fomentar la transparencia y eficiencia en la elaboración y observancia de normas oficiales mexicanas y normas mexicanas.
♣ Instituir la Comisión Nacional de Normalización para que coadyuve en las actividades que sobre normalización corresponde realizar a las distintas dependencias de la administración pública federal.
♣ Establecer un procedimiento uniforme para la elaboración de normas oficiales mexicanas por las dependencias de la administración pública federal.
♣ Promover la concurrencia de los sectores público, privado, científico y de consumidores en la elaboración y observancia de normas oficiales mexicanas y normas mexicanas.
♣ Coordinar las actividades de normalización, certificación, verificación y laboratorios de prueba de las dependencias de administración pública federal.
♣ Establecer el sistema nacional de acreditamiento de organismos de normalización y de certificación, unidades de verificación y de laboratorios de prueba y de calibración.

Las normas mexicanas son elaboradas por los organismos nacionales de normalización, y a falta de éstos, será la Secretaría de Economía la responsable de su elaboración, en términos de lo dispuesto por los artículos 51-A y 51-B de la Ley Federal sobre Metrología y Normalización.

Es necesario resaltar que las normas mexicanas son de aplicación voluntaria, salvo en los casos en que los particulares manifiesten que sus productos, procesos o servicios son conformes con las mismas y sin perjuicio de que las dependencias requieran en una norma oficial mexicana su observancia para fines determinados. El campo de aplicación de estas normas puede ser nacional, regional o local.

Existen algunos distribuidores de tecnología biométrica en México que aseguran cumplir con la Norma Oficial Mexicana, sin embargo, no existe una NOM que abarque las reglas, especificaciones y atributos que deben cumplir estas tecnologías por separado o en conjunto. Las características que los distribuidores de este tipo de tecnología ofrecen a los consumidores abarcan características de suministro de voltaje y corriente, temperatura, humedad, las funciones para las cuales fue diseñada la tecnología, sus aplicaciones, y las normas que estos productos cumplen, que en su mayoría son normas Internacionales, por

ejemplo normas de Comunicación como la FCC (Federal Comunications Commission) o de calidad como la ISO 9000, mas nunca se mencionan los estándares internacionales y/o nacionales bajo los cuáles son creados y distribuidos los productos.

CAPÍTULO V

Propuesta de Estándar

V.1. Justificación.

El uso cada vez más frecuente de las diferentes tecnologías biométricas que existen en el mercado, ya sea para uso empresarial o personal, ha llevado a los estándares a jugar un papel muy importante dentro de la Industria de la Biometría. Es a través de estos estándares que los desarrolladores y los usuarios finales le darán un mejor uso a la tecnología y sistemas biométricos creados. El uso correcto de los estándares biométricos proporciona además, un ambiente estable y de calidad a los consumidores e inversionistas.

En el capítulo IV se hizo referencia a varias de las organizaciones internacionales que se han dedicado a elaborar estándares biométricos en la última década, cada uno de los cuales cubre un aspecto y/o necesidad diferente de la industria biométrica. De igual forma se hizo referencia a dos organismos mexicanos, la NOM y la AMBI, dedicados a la elaboración de normas y estándares biométricos respectivamente. No obstante, estos organismos no han participado hasta el momento en el desarrollo de normas o estándares biométricos que puedan aplicarse no sólo a la tecnología internacional que se importa sino también a la que se desarrolla en el país.

Debido a la falta de información que sobre estándares biométricos existe en el país, así como al incremento en la utilización de dicha tecnología, es que se plantea la siguiente propuesta de estándar para el uso seguro de las tecnologías biométricas en el procesamiento de información.

V.2. Desarrollo de la Propuesta.

V.2.1. Introducción.

La Seguridad es uno de los aspectos más importantes en los actuales Sistemas de Información. Es por ello que se ha vuelto una necesidad la creación de metodologías para evaluar el grado de seguridad disponible en un sistema determinado. Se ha realizado mucho trabajo al respecto siendo una de las metodologías más importantes los Criterios Comunes (Common Criteria, CC), que son utilizados como base para la evaluación de las propiedades de seguridad de los productos y sistemas de las Tecnologías de Información (Information Technologies, IT). Los CC proveen un conjunto de requerimientos funcionales de seguridad para Tecnologías de Información que permiten establecer niveles de confianza. Un objetivo importante de las evaluaciones de los CC es que ayuda a los consumidores a determinar si un producto es suficientemente seguro para el uso al que está dirigido y si los riesgos implícitos son tolerables. Los Criterios Comunes están destinados a satisfacer: la confidencialidad, la integrad, la autenticidad y el control de acceso.

El uso de tecnología biométrica como medida de seguridad para proteger la información ha ido en aumento durante la última década. Empresas, bancos, aeropuertos y escuelas son un ejemplo de las áreas en donde se hace uso de este tipo de tecnología. Sin embargo, estos sistemas trabajan con información sensible, relativa a la identidad de un individuo, por lo que es necesario que de igual forma se realice una evaluación del grado de seguridad alcanzado por este tipo de tecnologías. La evaluación de los productos de tecnología biométrica no está explícita bajo la versión actual de los CC (v3.1). La implementación exitosa de estos productos depende de la naturaleza de la aplicación, localización y factores ambientales, demografía de la población de usuarios entre otras variables. Tomando en cuenta estos factores es que desarrolla la siguiente propuesta de estándar.

V.2.2. Propósito y Alcance.

La propuesta de estándar tiene por objetivo proporcionar una guía para asegurar el uso óptimo y seguro de las tecnologías biométricas más utilizadas en el procesamiento de información, enfatizando la parte de seguridad de los factores que intervienen (Hardware, Software, Organizacional) y que son determinantes para un buen manejo y resguardo de la información de una organización o particular.

La propuesta de estándar para el uso seguro de tecnologías biométricas en el procesamiento de información describe las acciones mínimas a llevarse a cabo por una organización o particular para asegurar el uso óptimo y seguro de las mismas por parte de los usuarios.

V.2.3. Sistemas Biométricos. Características Generales.

1. Los componentes principales de un sistema biométrico y que se explican con detalle más adelante son:

a) Captura: Adquisición de la muestra biométrica.

b) Extracción: Conversión de los datos biométricos a una forma intermedia (forma digital).

c) Crear Patrón: Conversión de los datos intermedios en un patrón de usuario para su almacenamiento.

d) Comparación: Cortejo que se hace con la información almacenada en el patrón de referencia.

2. Los sistemas Biométricos se separan en dos módulos. El primer módulo, el módulo de inscripción, se usa en cada nuevo usuario para tomar las muestras biométricas y establecer un nuevo patrón. El segundo módulo, el módulo de Identificación, toma las muestras nuevas y las compara con los patrones guardados de usuarios inscritos.

V.2.3.1. Captura.

3. Este componente se define como la captura automática o medición de las características físicas o del comportamiento de un individuo.

4. El mecanismo de captura puede incluir los procesos que realzan la calidad de la muestra adquirida tales como el uso de un número de adquisiciones para producir la muestra biométrica.

5. Cada tipo de dispositivo biométrico tendrá ciertos criterios y procedimientos definidos para el proceso de captura, tanto para la inscripción como para la verificación, por lo que éstos deberán estar redactados de manera entendible para los usuarios.

V.2.3.2. Extracción.

6. Este componente extrae y preserva las características biométricas de la muestra capturada. Es un componente crítico desde el punto de vista de la evaluación de la seguridad debido a que el nivel de unicidad inherente en un patrón puede influenciar el FRM del sistema.

7. El componente de extracción es generalmente un algoritmo de propietario. Inherente en este algoritmo se encuentra el control de calidad; mecanismo a través del cual se evalúa la calidad de la muestra. Si ésta no es aceptable, el proceso de captura puede ser repetido.

8. Se espera que los estándares de calidad del biométrico capturado sean altos durante el proceso de inscripción, puesto que éstos forman la base contra la que se harán las futuras comparaciones biométricas. Varios intentos pueden ser requeridos en el proceso de inscripción para que el mejor biométrico sea utilizado como referencia.

V.2.3.3. Creación del Patrón.

9. Este componente crea el patrón biométrico a partir de la información recopilada y almacenada por el componente de extracción. Éste puede incluir la encriptación de los biométricos y otra información personal del usuario.

V.2.3.4. Comparación.

10. Este componente compara la información biométrica extraída de la muestra con la información biométrica en el patrón de referencia.

11. La comparación puede ser contra un solo patrón (para verificación) o contra una lista de patrones candidatos (para identificación).

12. El umbral de comparación puede ser configurado por el administrador o puede ser fijado por el sistema biométrico. Claramente las medidas de seguridad relacionados con el ajuste de este valor, los medios de protección dentro del sistema biométrico para

salvaguardar el ajuste del umbral y el proceso de decisión interna para resolver, son algunos de los componentes más críticos de un sistema biométrico y sus vulnerabilidades deben ser cuidadosamente determinadas.

V.2.3.5. Otros componentes.

Transmisión y Almacenamiento.

13. La transmisión y almacenamiento de una muestra biométrica y otra información del usuario debe ser protegida mediante técnicas criptográficas. La integridad de la información biométrica puede ser mantenida con el uso de firmas digitales.

14. Los patrones pueden ser almacenados localmente dentro del sistema biométrico, en una base de datos separada o en un token dado al usuario como puede ser una smartcard.

15. Algunos sistemas biométricos pueden utilizar la compresión y descompresión de la información biométrica para facilitar su transmisión. En este caso habrá implicaciones de seguridad si el proceso de compresión resulta en una pérdida de información.

V.2.4. Seguridad Física y ambiental de los dispositivos biométricos.

16. El desempeño de un dispositivo biométrico puede verse afectado por las condiciones físicas del ambiente en que opere. Por ejemplo, el reconocimiento de iris depende de los niveles de iluminación, el reconocimiento de voz depende de los sonidos del ambiente y el polvo puede afectar a los dispositivos de huella dactilar.

17. Por esta razón, los dispositivos biométricos deben ser probados bajo varias condiciones ambientales. Los resultados de estas pruebas de “robustez física” pueden conducir a restricciones de uso en una localización.

18. Algunos de estos factores ambientales y su relevancia para tipos específicos de sistemas biométricos se muestran en la tabla 5.1.

	Iris y Retina	Rostro	Voz	Mano	Huella Dactilar (sensor óptico)
Niveles de sonido ambiente			X		
Polvo	X	X		X	X
Variaciones de voltaje	X	X	X	X	X
Humedad atmosférica					X
Vibraciones	X	X	X	X	X
Ruido electromagnético	X	X	X	X	X
Temperatura				X	X

Tabla 5.1 Factores ambientales relacionados a sistemas biométricos.

19. Debe notarse que los factores ambientales pueden influir tanto en los usuarios como directamente en los sensores de hardware de los dispositivos. Por ejemplo, la temperatura elevada o humedad pueden afectar los sensores de huella dactilar, pues los niveles de sudoración del usuario aumentan.

20. Cualquier restricción en las condiciones ambientales que afecten los dispositivos biométricos deberá ser debidamente documentada en las especificaciones del hardware o en la guía de usuario.

21. El envejecimiento de los sensores utilizados por los dispositivos biométricos puede deteriorar con el tiempo la robustez de los mismos. Esto significa que las pruebas físicas y ambientales se deberán llevar de forma periódica.

22. Los dispositivos biométricos se deben mantener alejados del humo, polvo, fuego y temperaturas extremas.

23. Así mismo los dispositivos biométricos deben estar fuera del alcance de vibraciones, insectos, ruido eléctrico, agua y rayos solares.

24. El área donde se encuentren instalados los dispositivos biométricos deberá mantener las condiciones de higiene adecuadas.

V.2.5. Seguridad ligada a los usuarios.

25. Uno de los factores más importantes a la hora de gestionar la seguridad de la información sin importar el tipo de IT del que se haga uso es el factor humano. De manera frecuente se observa que este factor es pasado por alto o menospreciado sin tomar en cuenta que a través del mismo se pueden reducir riesgos de error, hurto o mal uso por parte del recurso humano.

26. Los acuerdos de confidencialidad, la selección rigurosa del personal y la inclusión de la seguridad dentro de las responsabilidades contractuales son prácticas que ayudarán a reducir el riesgo del factor humano debido a errores, pérdidas, robos y uso indebido de la información.

27. Un programa de capacitación para el uso correcto de los dispositivos biométricos en uso, se debe proporcionar a todos los usuarios para asegurarse que éstos estén enterados de las amenazas y las medidas preventivas que deben tomar y así reducir al mínimo los riesgos de seguridad posibles.

28. Los incidentes, hechos sospechosos o que hayan sido observados deben divulgarse lo más pronto posible de modo que todos los integrantes de la cadena de responsabilidad sepan qué han de hacer y a quién informar en todo momento. Con estos se busca reducir al mínimo el daño ocasionado por percances y malos funcionamientos de la seguridad, así como aprender de tales incidentes.

29. El administrador del sistema biométrico podrá deshabilitar los patrones biométricos que no sean vigentes. Únicamente los miembros vigentes de la organización o comunidad donde se haga uso de los sistemas biométricos podrán tener acceso a los activos.

V.2.6. Vulnerabilidades de los sistemas biométricos.

30. Las pruebas de vulnerabilidad son una parte esencial para el buen funcionamiento de los dispositivos biométricos pues ofrecen información valiosa sobre el nivel de exposición que se tiene a las amenazas. La realización continua de evaluaciones a los dispositivos biométricos ayudará a fortalecer de manera anticipada su entorno frente a posibles amenazas.

31. Es particularmente importante considerar amenazas asociadas con la entrada y salida de los patrones biométricos.

32. Los patrones son considerados como información sensible pues identifican y están ligados a los individuos. El patrón es usado para determinar los derechos y privilegios del usuario para acceder a un recurso. Antes de que el patrón sea relacionado a las credenciales, privilegios y derechos se encuentra en su estado más vulnerable pues un atacante puede tratar de sustituir su propio patrón enmascarándolo como el usuario previsto.

33. Cuando un patrón es desasociado de su vínculo con el usuario, existe la posibilidad de un ataque de sustitución. Si el patrón sin vínculo es transportado o transmitido a través de un medio accesible y sin protección, se debe considerar un medio de protección adecuado. La posibilidad de duplicar el formato específico del dispositivo también debe ser considerada en la evaluación. Esto se debe hacer a través del análisis de los algoritmos que transforman la característica biométrica en el patrón usado por el dispositivo de comparación, determinando la salida del algoritmo y después determinando la probabilidad de duplicar la salida a través de algunos medios.

34. El camino que recorren los patrones dentro del sistema biométrico y entre el mismo sistema y el dispositivo externo se debe comportar de tal forma que sea imposible (o al menos excesivamente costoso) para el atacante capturar la información en cualquier punto del recorrido. Este punto es crítico si es que el sistema biométrico incluye el almacenamiento o transmisión de los patrones biométricos fuera del ambiente protegido.

35. Al realizar la evaluación de vulnerabilidad de un sistema biométrico, el evaluador debe considerar una amplia variedad de amenazas genéricas para la seguridad del sistema. Todos los elementos de un sistema biométrico son susceptibles a estas amenazas en algún grado.

36. En la tabla 5.2 se muestran las amenazas generales que deben ser consideradas por los administradores, desarrolladores y diseñadores de sistemas biométricos, al evaluar las vulnerabilidades de los mismos.

Amenazas
1. Amenazas de Usuario. Usuarios autorizados proveen su información biométrica sin saberlo, bajo amenaza o con toda la intención, a un impostor.
1.1 El impostor captura la muestra biométrica de un usuario autorizado. Por ejemplo: la fotografía de su cara o la grabación de su voz.
1.2. El impostor roba la información biométrica de un usuario autorizado.
1.3. Un usuario autorizado provee de manera voluntaria su información biométrica al impostor.
1.4. Un usuario autorizado modifica su información biométrica para facilitar un ataque por parte del impostor.
2. Amenazas de Usuario/Captura de muestra biométrica.
2.1. El impostor presenta una muestra biométrica artificial (ejemplos: huella digital de gelatina, grabación de voz) en un intento por hacerse pasar por un usuario autorizado.
2.2. El impostor presenta una muestra biométrica de baja o nula calidad en un esfuerzo por coincidir con una muestra biométrica débil o de baja calidad.
2.3. El impostor utiliza una imagen biométrica residual dejada en el sistema biométrico (típicamente una huella dactilar latente) en un intento por hacerse pasar por el último usuario autorizado.
2.4. El impostor presenta su propia muestra biométrica después de que ésta ha sido: a) Proporcionada en una tarjeta inteligente personal. b) Colocada en la base de datos del sistema biométrico en una inscripción ilegal. c) Ilegalmente insertada en el subsistema de comparación del sistema biométrico.
3. Amenazas de Captura/Extracción.
3.1. El impostor intercepta una muestra biométrica autorizada durante la transmisión entre los subsistemas de Captura y Extracción.
3.2. El impostor inserta una muestra biométrica autorizada directamente en el subsistema de Extracción.
4. Amenazas de Extracción/Comparación durante la Verificación.
4.1. El impostor intercepta las características biométricas extraídas durante la transmisión entre los subsistemas de Extracción y Comparación.
4.2. El impostor inserta las características biométricas extraídas directamente en el subsistema de Comparación.
5. Amenazas de Extracción/Almacenamiento de la muestra durante la Inscripción.
5.1.Un usuario autorizado presenta una muestra biométrica de baja calidad, con ruido y variaciones o presenta una muestra artificial en un intento por crear y almacenar un

patrón biométrico débil
5.2. Un usuario no autorizado queda registrado por: a) Un error del administrador. b) El patrón de un usuario autorizado fue interceptado y reemplazado por el patrón del impostor.
6. Amenazas de almacenamiento del Patrón.
6.1. El impostor roba el patrón biométrico de un usuario autorizado del medio de almacenamiento o de otro sistema biométrico.
6.2. El atacante modifica o elimina los patrones biométricos en almacenamiento.
6.3. El impostor intercepta el patrón biométrico autorizado durante la transmisión entre los subsistemas de Extracción y Almacenamiento del Patrón.
7. Amenazas en la recuperación del patrón.
7.1. El impostor intercepta una muestra biométrica autorizada durante la transmisión entre los subsistemas de Almacenamiento del Patrón y Comparación.
7.2. El impostor inserta su propio patrón directamente en el subsistema de Comparación.
8. Amenazas de Administración y Manejo de recursos.
8.1. Un usuario autorizado hostil puede adquirir privilegios de administrador a través de medios no biométricos (password o sistema de respaldo) y de esta forma puede modificar el umbral de comparación, modificar los privilegios de los usuarios, permitir el acceso no autorizado a los patrones almacenados, inscribir un usuario no autorizado.
9. Amenazas al sistema biométrico.
9.1. El atacante corta la fuente de energía del sistema biométrico.
9.2. El atacante gana acceso no autorizado a los privilegios con o sin ayuda de un usuario autorizado después de que el usuario ha sido autenticado.
9.3. Un usuario gana acceso a privilegios no autorizados después que los privilegios han sido inapropiadamente modificados.
10. Amenazas a los componentes de Hardware.
10.1. El atacante trata de forzar, modificar o desactivar uno o más componentes de hardware.
10.2. El atacante intercepta/inserta patrones biométricos autorizados de/hacia uno o más componentes de Hardware.
10.3. El atacante explota los defectos del diseño, condiciones ambientales o modo de fallo.
10.4. El atacante “inunda” uno o más componentes del hardware con ruido, por ejemplo energía electromagnética o acústica.
11. Amenazas al software.
11.1. El atacante trata de forzar, modificar o desactivar uno o más archivos ejecutables del software.
11.2. El atacante explota los defectos del diseño y modo de fallo del software.
11.3. Un virus u otro software malicioso es introducido en el sistema biométrico.
11.4. Un impostor intercepta/inserta patrones biométricos autorizados de/hacia uno o más componentes de software.
12. Amenazas a las conexiones (incluidas las amenazas de red).

12.1. El atacante trata de forzar, modificar o desactivar una o más conexiones entre los componentes.
12.2. El impostor intercepta o inserta muestras biométricas o patrones autorizados mientras están siendo transmitidos entre subsistemas o componentes.

Tabla 5.2. Amenazas Generales de los Sistemas Biométricos.

V.2.7. Pruebas de funcionamiento de Dispositivos Biométricos.

37. La meta de la prueba de funcionamiento de un dispositivo biométrico es ayudar a la empresa o particular a seleccionar y configurar el dispositivo más rentable para una aplicación determinada y ayudar al usuario actual a mejorar el funcionamiento del dispositivo biométrico en una aplicación específica.

38. Cada tecnología biométrica tiene fuerzas y debilidades dependiendo de la aplicación en la cual se utiliza. Se deben probar y seleccionar los dispositivos con una aplicación en mente y sin poner en riesgo la integridad física del usuario.

39. Todas las aplicaciones biométricas se pueden clasificar en seis categorías:

a) Atendido contra No Atendido: Esta categoría hace referencia a si el uso del dispositivo biométrico durante la operación será observado y dirigido por la gerencia del sistema. Las aplicaciones no cooperativas requerirán generalmente la operación supervisada, mientras que la operación cooperativa puede o no serlo.

b) Público contra Privado: Los usuarios del sistema biométrico serán clientes de la empresa (público) o los empleados de la misma (privado). Las actitudes hacia el uso de los dispositivos, que afectarán directamente el funcionamiento, varían claramente al depender del lazo entre los usuarios finales y la administración del sistema.

c) Habituado contra no Habituado: Esta categoría se aplica a los usuarios previstos de la aplicación. Los usuarios que presentan un rasgo biométrico diariamente pueden ser considerados habituados después del periodo inicial de uso. Los usuarios que no han presentado el rasgo recientemente pueden ser considerados no-habituados.

d) Cooperativa contra no Cooperativa: Se refiere al comportamiento del usuario fraudulento en las aplicaciones que verifican la demanda positiva de identificación. Este usuario está cooperando con el sistema en la tentativa de ser reconocido como alguien que no es. A eso se le llama una aplicación cooperativa. En las aplicaciones que verifican una demanda negativa a la identidad, el usuario fraudulento está procurando no cooperar con el sistema en una tentativa de no ser identificado. A esto se le conoce como una aplicación no cooperativa.

A los usuarios de aplicaciones cooperativas se les puede pedir identificarse de una cierta manera, por ejemplo con una tarjeta.

e) Descubierto o Encubierto: Si el usuario está enterado que se está midiendo un identificador biométrico, el uso es Descubierto. Si es inconsciente, el uso es secreto o encubierto.

f) Abierto contra Cerrado: El sistema será requerido para intercambiar datos con otros sistemas biométricos administrados por otra gerencia. Por ejemplo, el FBI deseará intercambiar la información de la huella dactilar con las agencias locales de policía, requiriendo por lo tanto de un sistema abierto. Si un sistema es abierto, se requiere que se usen ciertos estándares en la colección de datos y en la transmisión.

V.2.8. Bibliografía.

[1] Common Criteria "Evaluation Methodology", v.2.3, August 2005.
http://www.commoncriteriaportal.org/

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security Functional Requirements, v.2.1, August 1999.
http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF

[3] "Biometric Evaluation Methodology Supplement (BEM)", v.1.0 – 2002.
http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

[4] Best Practices in Testing and Reporting Performance of Biometric Devices, Tony Mansfield and Jim Wayman for the UK Biometrics Working Group, NPL Report CMSC 1402, Version 2, August 2002.
http://www.cesg.gov.uk/technology/biometrics/media/Best Practice.pdf

[5] UNE-ISO/IEC 17799, "Código de Buenas prácticas para la Gestión de la Seguridad de la Información", 2002.
http://www.criptored.upm.es/guiateoria/gt_m209d.htm

V.2.9. Definiciones y Abreviaciones.

Aplicación Biométrica: Uso que se la da a un sistema Biométrico.

Amenaza: Todo aquello que intenta o pretende destruir, las amenazas provienen de diversas fuentes.

Biometría: Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de los vocablos griegos *bios* (vida) y *metron* (medida).

Característica Biométrica: Representación de una muestra biométrica extraída por el sistema de captura.

CC: Common Criteria (Criterios Comunes); esquema internacional para la evaluación y certificación de la seguridad de sistemas de Tecnologías de la Información.

Confidencialidad: Capacidad de asegurar que sólo las personas, sistemas o procesos autorizados puedan tener acceso a la información.

Hardware: Conjunto de componentes que integran la parte física de una computadora (teclado, mouse, monitor, etc).

Impostor: Persona que reclama una identidad que no le pertenece.

Información Biométrica: Información extraída de una muestra biométrica; usada para crear un patrón.

Inscripción: Proceso mediante el cual se captura la muestra biométrica de un usuario y se lleva a cabo el proceso de almacenamiento de los patrones e información asociados a la identidad de ese usuario.

IT: Tecnología de la Información.

Muestra Biométrica: Medida biométrica presentada por el usuario o capturada por el sistema de colección de datos.

Patrón: Información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

Seguridad: Confianza, tranquilidad, certidumbre procedente de la idea de que no hay peligro que temer, todo está bien.

Sensor: Dispositivo que detecta una acción externa, temperatura, presión, entre otras, y la transmite adecuadamente.

Sistema Biométrico: Método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas.

Smartcard: Tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Token: Es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.
Umbral: Valor paramétrico usado para convertir un valor de coincidencia en una decisión.

Usuario: Individuo que requiere acceder a cierta información o cierto lugar protegido por un sistema biométrico.

Vulnerabilidad: Debilidad que puede ser explotada para violar la seguridad.

CAPÍTULO VI

Difusión de la Tecnología

VI.1. Introducción.

Desde siempre, el hombre ha tenido la necesidad de comunicarse con los demás, de expresar pensamientos, ideas, emociones; de dejar huella de sí mismo. Así, también se reconoce en el ser humano la necesidad de buscar, de saber, de obtener información creada, expresada y transmitida por otros. La creación, búsqueda y obtención de información son pues acciones esenciales a la naturaleza humana. La búsqueda constante del hombre por satisfacer cada vez mejor su necesidad de comunicación ha sido el impulso que ha logrado la instauración en el mundo de instrumentos cada día más poderosos y veloces en el proceso comunicativo. Sólo basta una retrospectiva para definir cómo el ser humano ha logrado evolucionar sus formas de comunicación: Desde rudimentarios métodos como la escritura jeroglífica, pasando por la invención del alfabeto y del papel, dando un leve salto hasta la llegada de la imprenta, y apenas uno más para la aparición del teléfono, el cine, la radio y la televisión. Todos estos instrumentos han sido ciertamente un avance en las formas de comunicación del hombre y, prácticamente todos, han sido posibles gracias a la tecnología, que a su vez ha sido el instrumento cuya evolución ha determinado el avance de la humanidad.

Dentro de estos avances tecnológicos se encuentra Internet, que destaca particularmente porque se trata de un sistema integral que facilita a las personas el rápido acceso a cantidades infinitas de información, a un costo relativamente bajo, sobre cualquier índole y proveniente de cualquier rincón del mundo. Internet ha cambiado y mejorado diversos procesos, ha logrado unir al mundo en cuanto a su capacidad de conexión y representa sin duda una oportunidad para nuevas creaciones.

Debido al gran poder de divulgación que posee Internet, a su fácil accesibilidad y manejo, y debido también a la falta de conocimiento que sobre el tema de Biometría Informática se tiene en México, se decidió, como parte de este trabajo de Tesis, crear un espacio en Internet por medio del cual se difunda la información recopilada a lo largo de esta investigación. Esto se llevará a cabo a través de una de las diferentes alternativas tecnológicas de que se puede hacer uso en internet como son los blogs, los foros, los sitios web, entre otros. De esta forma las personas interesadas en este tema y también las que no están familiarizadas con él, podrán conocer y aprender un poco más sobre el mismo y podrán también mantenerse informadas acerca de los avances tecnológicos que en materia de biometría se producen en México y en el mundo.

VI.2. Alternativas tecnológicas.

VI.2.1. Páginas Web.

Una página Web es un documento electrónico que tiene como finalidad mostrar información en la WWW (World Wide Web). Una página puede estar relacionada con una

o más páginas. Es decir; un conjunto de páginas de un solo tema forman un Sitio; y a su vez un conjunto de Sitios que ofrecen uno o más servicios forman un Portal.

Una página web tiene contenido que puede ser visto o escuchado por el usuario final, estos elementos incluyen: Texto, Imágenes, Video, Audio, Enlaces, Listas, Tablas, Formularios, entre otros. La página web también puede traer contenido que es interpretado de forma diferente dependiendo del navegador y generalmente no es mostrado al usuario final, estos elementos incluyen: Hojas de Estilo (CSS – Cascading Style Sheets), Scripts y Meta Tags. El contenido de las páginas web se puede visualizar con ayuda de un programa, regularmente conocido como navegador; el cual puede tener una interfaz gráfica o una interfaz en modo texto. Los navegadores más utilizados son el Internet Explorer de Microsoft y el Mozilla de Firefox.

Para crear una página web, es necesario un editor de texto o un editor de HTML (HyperText Markup Language), que es lenguaje de marcado predominante en la construcción de páginas web. Anteriormente para crear una página web, era necesario tener conocimientos de los códigos propios del lenguaje HTML, que aunque no son complejos, resultaban confusos y de difícil manejo para un usuario de nivel básico. Sin embargo, hoy en día, existen en el mercado distintos programas creados específicamente para facilitar el diseño de Sitios Web. Estos editores de texto, también conocidos como editores “WYSIWYG” (What You See Is What You Get) permiten a los usuarios crear las páginas web de forma visual, es decir; los cambios que hacen se ven en tiempo real, casi igual como se ve en el navegador. Algunos de estos programas son: Dreamweaver, Amaya y WebFácil.

El diseño de una página web es completamente personal. Éste se puede hacer de acuerdo con las preferencias personales del diseñador o se puede utilizar una plantilla. Una vez terminada la página web, se puede publicar en la WWW de dos formas; la primera es a través de un Servidor Web, el cual servirá de Host. La otra forma de publicar una página web es utilizando sitios que ofrecen hospedaje gratuito a cambio de un espacio limitado y publicidad, ejemplos de estos sitios son: Geocities de Yahoo, Tripod o Angelfire.
Sin importar de qué manera se publique una página web, ésta es solicitada y transferida de los servidores usando el Protocolo de Transferencia de Hipertexto (HTTP – HyperText Transfer Protocol).

VI.2.2. Blogs.

Un blog es un sitio web periódicamente actualizado que recopila cronológicamente textos o artículos de uno o varios autores, apareciendo primero el más reciente, donde el autor conserva siempre la libertad de dejar publicado lo que crea pertinente. El uso o tema de cada blog es particular, los hay de tipo personal, periodístico, empresarial o corporativo, tecnológico, educativo (edublogs), político, entre otros.
Los primeros blogs eran simplemente componentes actualizados de sitios web comunes. Sin embargo, la evolución de las herramientas que facilitaban la producción y

mantenimiento de artículos web publicados y ordenados de forma cronológica hizo que el proceso de publicación pudiera dirigirse hacia muchas más personas.
Los blogs pueden ser almacenados mediante servicios de alojamiento de blogs dedicados o pueden ser utilizados mediante software para blogs, o mediante servicios de alojamiento web corrientes.

Existen varias herramientas de mantenimiento de blogs que permiten, sin necesidad de elevados conocimientos técnicos, administrar todo el blog, coordinar, borrar o reescribir los artículos, moderar los comentarios de los lectores, etc., de una forma casi tan sencilla como administrar el correo electrónico. Actualmente su modo de uso se ha simplificado a tal punto que casi cualquier usuario es capaz de crear y administrar un blog.
Estas herramientas de mantenimiento se clasifican, principalmente, en dos tipos: aquellas que ofrecen una solución completa de alojamiento, gratuita (como Freewebs, Blogger y LiveJournal), y aquellas soluciones consistentes en software que, al ser instalado en un sitio web, permiten crear, editar y administrar un blog directamente en el servidor que aloja el sitio (como es el caso de WordPress o de Movable Type). Este software es una variante de las herramientas llamadas Sistemas de Gestión de Contenido (CMS), y muchos son gratuitos.

Las herramientas que proporcionan alojamiento gratuito asignan al usuario una dirección web (por ejemplo, en el caso de Blogger, la dirección asignada termina en "blogspot.com"), y le proveen de una interfaz, a través de la cual puede añadir y editar contenido. Sin embargo, la funcionalidad de un blog creado con una de estas herramientas se limita a lo que pueda ofrecer el proveedor del servicio, o hosting. Un software que gestione el contenido, en tanto, requiere necesariamente de un servidor propio para ser instalado, del modo en que se hace en un sitio web tradicional. Su gran ventaja es que permite control total sobre la funcionalidad que ofrezca el blog, permitiendo así adaptarlo totalmente a las necesidades del sitio, e incluso combinarlo con otros tipos de contenido.

Es importante destacar que el aspecto más importante de los blogs es su interactividad, especialmente en comparación con páginas web tradicionales. Dado que se actualizan frecuentemente y permiten a los visitantes responder a las entradas, los blogs funcionan a menudo como herramientas sociales, para conocer a personas que se dedican a temas similares; con lo cual en muchas ocasiones llegan a ser considerados como una comunidad.

VI.2.3. Foros.

Un foro en internet, también conocido como foro de opinión o foro de discusión, es una aplicación web que le da soporte a discusiones u opiniones en línea. Por lo general los foros en Internet existen como un complemento a un sitio web invitando a los usuarios a discutir o compartir información relevante a la temática del sitio, en discusión libre e

informal, con lo cual se llega a formar una comunidad en torno a un interés común. Las discusiones suelen ser moderadas por un coordinador o dinamizador quien generalmente introduce el tema, formula la primera pregunta, estimula y guía, sin presionar, otorga la palabra, pide fundamentaciones y explicaciones y sintetiza lo expuesto antes de cerrar la discusión.

La forma de ver un foro puede ser llana, en la que las respuestas de una discusión se ordenan en forma cronológica; o puede ser anidada, en la que cada respuesta está vinculada con el mensaje original o alguna de las respuestas subsiguientes formando algo así como un árbol genealógico de discusión. Por lo general los foros disponen de formas de personalizar la apariencia a la que le resulte más cómoda al usuario e inclusive algunas formas mixtas.

Por lo general los foros están desarrollados en PHP, Perl, ASP.NET o Java. Los datos y la configuración se guardan, generalmente en una base de datos o una serie de archivos de texto. Cada versión provee funciones o capacidades diferentes: los más básicos se limitan a los mensajes sólo con texto, los más avanzados facilitan la inclusión de multimedia, formato del texto y HTML. Algunos sistemas de foros son: phpBB, vBulletin, Invision power board, MyBB, SMF, YaBB, Ikonboard, UBB, JavaBB y otros.

Los principales enemigos contra el correcto funcionamiento del foro y que un moderador debe controlar, son el spam (la publicación de mensajes no solicitados, generalmente publicitarios, de forma caótica o que van en contra de las reglas del foro), los troles (usuarios cuyo único interés es molestar a otros usuarios e interrumpir el correcto desempeño del foro, ya sea por no estar de acuerdo con su temática o simplemente por divertirse de ese modo), y los leechers (usuarios que sólo desean aprovecharse). Además los foros también pueden sufrir ataques de Crackers.

Un dato interesante acerca de los foros es que muchos de éstos tienden a fomentar la creación de comunidades con reglas propias y, en algunos casos, incluso un propio lenguaje formando una subcultura. Se llegan a organizar eventos sociales que pueden llegar a involucrar viajes internacionales masivos.
Más allá de que son una herramienta en Internet, los foros generan una gran cantidad de escritos; pero en contraste con otras tecnologías modernas basadas en Internet, como la mensajería instantánea; muchos de los miembros de los foros realmente se preocupan por la calidad de los textos tanto en contenido como en redacción, ortografía, gramática y otras características del lenguaje escrito.

VI.2.4. Wiki.

Un wiki, o una wiki, es un sitio cuyas páginas web pueden ser editadas por múltiples usuarios a través del navegador. Los usuarios pueden crear, modificar o borrar un mismo texto que comparten. La mayoría de los wikis actuales conservan un historial de cambios

que permite recuperar fácilmente cualquier estado anterior y ver 'quién' hizo cada cambio. La famosa enciclopedia Wikipedia, la cual al día de hoy aglutina más de un millón de artículos en Inglés y 100,000 en español, es un ejemplo de un sitio wiki pues permite a los usuarios acceder y modificar sus contenidos.

La principal utilidad de un wiki es que permite crear y mejorar las páginas de forma instantánea, dando una gran libertad al usuario, y por medio de una interfaz muy simple. Esto hace que más gente participe en su edición, a diferencia de los sistemas tradicionales, donde resulta más difícil que los usuarios del sitio contribuyan a mejorarlo.

Una característica que define la tecnología wiki es la facilidad con que las páginas pueden ser creadas y actualizadas. En general no hace falta revisión para que los cambios sean aceptados. La mayoría de wikis están abiertos al público sin la necesidad de registrar una cuenta de usuario. A veces se requiere hacer login para obtener una cookie de *wiki-firma*, para autofirmar las ediciones propias. Otros wikis más privados requieren autenticación de usuario.

Existen varios programas, generalmente scripts de servidor en Perl o PHP, que implementan un wiki. Con frecuencia, suelen utilizar una base de datos, como MySQL. Estos programas suelen distinguirse por el destino (Uso personal, Intranet, Internet) y por la funcionalidad (opciones de seguridad, descarga de archivos, editores WYSIWYG, entre otros)

VI.3. Selección de la tecnología.

Para seleccionar el medio a través del cual se difundirá la información presentada en este trabajo de Tesis, se lleva a cabo un análisis de las diferentes alternativas tecnológicas presentadas anteriormente, tomando en cuenta el objetivo, el uso, las herramientas de programación y las características principales de cada tecnología. Este análisis se puede apreciar en la tabla 6.1.

Tecnología	Objetivo	Uso	Características Principales	Herramientas de Programación
Página Web	Mostrar información en la World Wide Web (WWW).	Personal, periodístico, educativo y empresarial, político, comercial, entre otros.	*El contenido de la página no debe ser actualizado constantemente. *La Información no sufre cambios por parte de los usuarios. *El sitio web se encuentra almacenado en un	*Lenguajes de Programación como HTML, PHP, JavaScript, ASP y JSP. *Editores de textos o de HTML como Notepad, Dreamweaver y Amaya, *Uso de

			servidor web.	Programas como Flash.
Blog	Mostrar textos, artículos, opiniones, críticas de uno o varios autores en la WWW.	Personal, periodístico, empresarial o corporativo, tecnológico, educativo, entre otros.	*El blog es actualizado de manera periódica. *Los usuarios pueden añadir comentarios a cada entrada publicada en el blog.	Lenguajes de programación como HTML, JavaScript y PHP.
Foro	Dar soporte en línea a discusiones u opiniones que se tengan sobre alguna temática en particular.	Recreativo.	*Puede ser el complemento de un sitio web. *Las discusiones son moderadas por un coordinador. *Los foros tienen a fomentar la creación de comunidades con reglas propias.	Lenguajes de Programación como PHP, ASP.NET, Perl o Java.
Wiki	Mostrar información en la World Wide Web (WWW).	Personal y educativo.	*El contenido de la información puede ser modificado por los usuarios y estos cambios se visualizan de manera instantánea.	*Lenguajes de Programación como PHP y Perl. *Uso de bases de datos como MySQL.

Tabla 6.1 Análisis de Alternativas Tecnológicas.

Con base en la información presentada en la tabla 6.1 para cada uno de los elementos que se tomaron en cuenta para realizar el análisis se concluyó que la mejor opción sería a través de una página web[1] debido a que lo que se pretende con este trabajo es informar a la comunidad estudiantil y docente de la Facultad de Ingeniería sobre el estado del arte que guarda la biometría a nivel internacional y nacional. Otro aspecto fundamental que se tomó en cuenta fue el uso y manejo de la información por parte de los usuarios; la principal ventaja de una página web es que ésta no requiere una actualización constante de la información como es el caso de un blog, la información tampoco estará sujeta a cambios por parte de los usuarios como en un wiki, sin embargo, los usuarios podrán hacer comentarios y/o sugerencias sobre el contenido y estructura de la página que serán tomados en cuenta para su mejoría.

[1] http://redyseguridad.fi-p.unam.mx/proyectos/biometria/index.html

VI.4. Diseño.

El diseño de la página web está basado en la Hoja de Estilo programada por el Ing. Antonio Moltalvo, misma que fue utilizada para la creación del Tutorial de Redes y Seguridad. El diseño consta de las siguientes secciones:

- Barra de Título, en la que se muestra el nombre y escudo de la institución educativa así el título general de la página.
- Sección de noticias e imágenes, en la que el usuario puede consultar, al inicio de cada capítulo, noticias relacionadas con el uso y avance de las diferentes tecnologías biométricas; mientras que en cada subtema se observan imágenes relacionadas con la información que en éste se presenta.
- Menú de Capítulo, que permite al usuario elegir el tema o subtema que desea consultar dependiendo del capítulo en que se encuentra.
- Marco de Información. En esta sección se presenta la información referente a cada tema y/o subtema.
- Barra de selección, en la que se encuentra un formato que permite a los usuarios elegir el capítulo que quieren consultar. En esta barra también se encuentran dos flechas de navegación que permiten avanzar o retroceder hacia cada subtema del capítulo en el que se encuentren.

Una muestra de la página web, se puede observar en la figura 6.1.

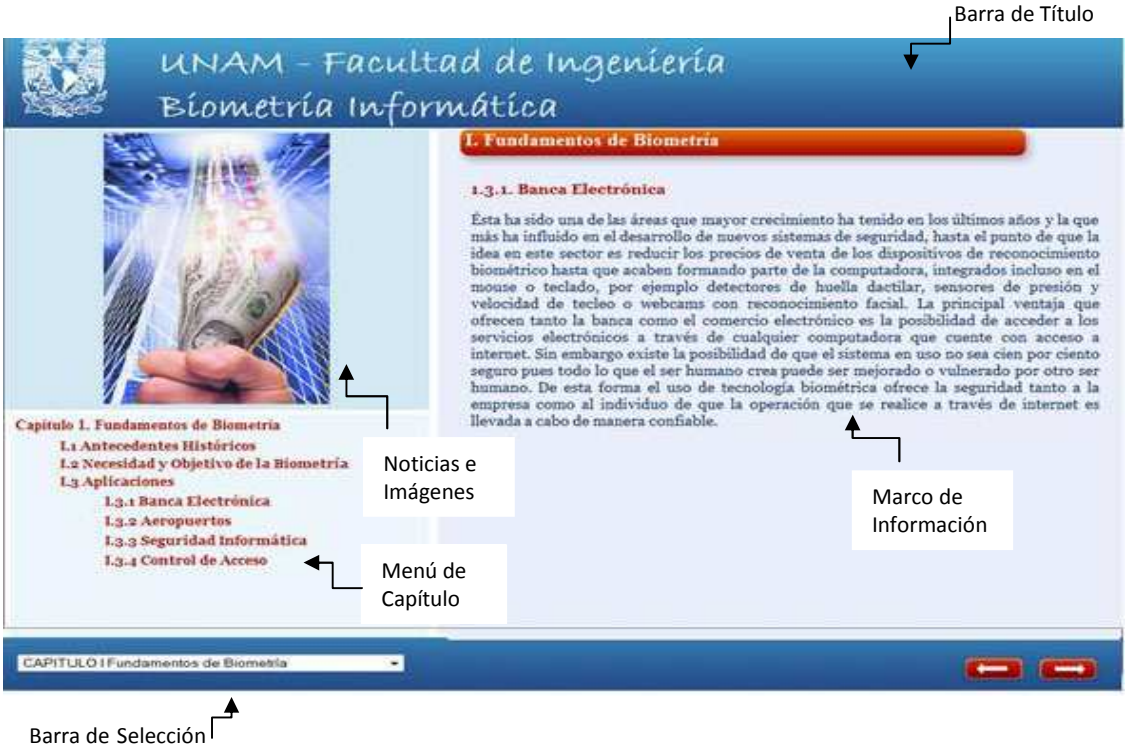


Figura 6.1. Página Web.

CONCLUSIONES

La presente tesis **Propuesta de Estándar para el uso seguro de Tecnologías Biométricas** busca ser una guía de ayuda para todas las personas interesadas en la Biometría Informática y el uso de estándares para este tipo de tecnologías sin importar el nivel de conocimientos que posean sobre el tema, mostrando los aspectos importantes que deben ser considerados, desde el desarrollo hasta la implementación, para darle un uso responsable, adecuado y seguro a los sistemas y tecnologías biométricas y siempre tomando en cuenta las necesidades y circunstancias que rodean a los individuos, empresas u organizaciones que harán uso de dichas tecnologías.

Implementar una metodología o estándar dentro de una organización proporciona un ambiente estable y de calidad a los consumidores e inversionistas así como un lenguaje mediante el cual éstos se pueden comunicar sin ambigüedades. De igual forma sirven como una "guía" para que los desarrolladores y usuarios finales le den un mejor uso a la tecnología y sistemas creados; sean estos de origen nacional o internacional.

Existen estándares biométricos que se encargan de regular diferentes aspectos de los sistemas biométricos. La gran mayoría de estos estándares han sido elaborados por instituciones internacionales, por ejemplo, ISO, BioAPI, NIST, entre muchos otros.
México ha incursionado en la importación y elaboración de tecnología y sistemas biométricos, debido a esto es necesario que los organismos nacionales de certificación se involucren en la elaboración de estándares que respalden los productos elaborados en el país.

Con esto como base, es que el presente trabajo se desarrolló buscando cubrir dos grandes aspectos: el primero, que como ya se ha mencionado, es la propuesta del estándar para el uso seguro de tecnologías biométricas, la cual ha sido ya entregada a la Dirección General de Normas (DGN), dependencia gubernamental adscrita a la Secretaría de Economía (SE) con fecha del 12 de Marzo de 2009 y número de folio 1282. La portada sellada de la propuesta de estándar se puede consultar en el Apéndice B del trabajo de tesis.
De igual manera se intentó hacer llegar la propuesta a la Asociación Mexicana de Biometría e Identidad (AMBI), sin embargo, no se obtuvo respuesta por parte de esta institución.

El otro aspecto también de gran interés para la comunidad en general y en particular para la de Ingeniería en Computación, es la difusión del conocimiento sobre sistemas biométricos, para lo cual se desarrolló un tutorial a través del cual la comunidad estudiantil y docente de la Facultad podrá mantenerse informada acerca de los avances tecnológicos que en materia de biometría se producen en México y en el mundo.

Finalmente, se espera que la propuesta de estándar desarrollada, además de ser tomada en cuenta, sea el primer escalón para que instituciones gubernamentales o de carácter privado emprendan las actividades necesarias para la elaboración de Normas Oficiales o Estándares Mexicanos que regulen el uso de tecnologías biométricas en el país y que los

profesionales de la seguridad en tecnologías de la información encuentren en el material publicado una apoyo en la adquisición de conocimientos en esta área de gran interés.

Glosario de Términos

Algoritmo: Un algoritmo es una serie de pasos organizados que describe el proceso que se debe seguir, para dar solución a un problema específico.

AMBI: Asociación Mexicana de Biometría e Identidad.

Amenaza: Todo aquello que intenta, puede o pretende destruir, las amenazas provienen de diversas fuentes.

Analógico: El término analógico se refiere a las magnitudes o valores que varían con el tiempo en forma continua como la distancia, la temperatura y la velocidad y que pueden representase en forma de ondas.

ANSI: American National Standars Institute. Es una organización privada sin fines de lucro, que permite la estandarización de productos, servicios, procesos, sistemas y personal en Estados Unidos.

API: Application Programming Interface. Conjunto de funciones y procedimientos que un sistema operativo, librería o servicio provee para dar soporte a los requerimientos hechos por programas de computadoras.

Base de datos: Es un conjunto de datos (no redundantes) relacionados entre sí.

Biometría: Es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de los vocablos griegos *bios* (vida) y *metron* (medida).

Biometría Dinámica: Es la rama de la Biometría que lleva a cabo la identificación de individuos basándose únicamente en las características de comportamiento intrínsecas.

Biometría Estática: Es la rama de la Biometría que lleva a cabo la identificación de individuos basándose únicamente en las características físicas intrínsecas.

Biometría Informática: Es el conjunto de métodos automatizados de identificación y verificación de la identidad de un individuo, mediante técnicas matemáticas auxiliadas por computadora, basándose en características conductuales o físicas propias del individuo.

CBEFF: Common Biometric Exchange File Format. Estándar cuyo objetivo es definir los formatos de los patrones biométricos para facilitar el acceso y el intercambio de diferentes tipos de datos biométricos a los sistemas que integran esta tecnología o entre diferentes componentes de un mismo sistema.

CC: Common Criteria (Criterios Comunes); esquema internacional para la evaluación y certificación de la seguridad de sistemas de Tecnologías de la Información.

CCD: Charge Coupled Device. Dispositivo que convierte una imagen óptica en una señal eléctrica.

CDSA / HRS: Common Data Security Architecture Specification / Human Recognition Services. Es una arquitectura que se encuentra parcialmente involucrada en el desarrollo de estándares biométricos, fue creada por Intel en Diciembre de 1997 con la participación de Netscape, JP Morgan, Shell, IBM, Motorola y HP.

Chat: Es un anglicismo que se refiere a una comunicación escrita a través de Internet entre dos o más personas que se realiza de manera instantánea. Esta comunicación puede ser llevada a cabo desde cualquier lado del mundo.

Cifrar: Es un proceso de conversión que se utiliza para ocultar un mensaje y evitar que sea legible si éste es accedido o interceptado por algún proceso o usuario no autorizados.

Clase: Conjunto de entidades que comparten alguna característica que las diferencia de otras.

Clave (criptografía): Es una pieza de información que controla la operación de un algoritmo criptográfico.

Confidencialidad: Capacidad de asegurar que sólo las personas, sistemas o procesos autorizados puedan tener acceso a la información.

Cracker: Persona que irrumpe dentro de un sistema de cómputo sin ser invitado e intenta romper las reglas para robar, destruir o alterar información.

Criptografía: Es la ciencia encargada de transformar la información de manera tal que ésta quede encubierta y sea incomprensible para todo aquél que no tenga la autorización correspondiente para acceder a ella. El término se deriva de los vocablos griegos *kryptós* (ocultar) y *graphé* (escribir).

Dactiloscopia: Ciencia que se encarga del estudio de las características de las huellas dactilares. Proviene de los vocablos griegos *daktilos* (dedos) y *skopein* (examen o estudio). Este nombre fue inventado por el doctor Francisco Latzina en sustitución al dado en 1892 por Sir Francis Galtón (Icnofalangometría).

Dato: Información dispuesta de manera adecuada para su tratamiento por una computadora.

Digital: El término digital se refiere a cantidades discretas como la cantidad de personas en un una sala, la cantidad de libros en una biblioteca o la cantidad de autos en una zona de estacionamiento.

Encriptar: Acción de proteger información para que no pueda ser leída sin una clave.

Estándar: Un estándar es un conjunto de reglas que deben cumplir los productos, procedimientos o investigaciones que afirmen ser compatibles con el mismo producto.

Estándar de facto: Un estándar de facto es aquella norma que se caracteriza por no haber sido consensuada ni legitimada por un organismo de estandarización. Por el contrario, se trata de una norma generalmente aceptada y ampliamente utilizada por iniciativa propia de un gran número de interesados.

FAR: False Acceptance Rate. Este parámetro hace referencia a la probabilidad de que un usuario no autorizado sea aceptado.

FCC: Federal Comunications Commission. Es una agencia estatal independiente de Estados Unidos, bajo responsabilidad directa del Congreso. La FCC fue creada en 1934 con la Ley de Comunicaciones y es la encargada de la regulación (incluyendo censura) de telecomunicaciones interestatales e internacionales por radio, televisión, redes inalámbricas, satélite y cable.

FRR: False Rejection Rate. El parámetro hace referencia a la probabilidad de que un usuario que está autorizado sea rechazado a la hora de intentar acceder al sistema.

HA-API: Human Authentication Application Program Interface. Este proyecto se divide en dos partes: la creación de una API biométrica genérica junto con la implementación de una prueba de concepto y la integración de la API en sistemas comerciales de autenticación que funcionan en red.

Hacker: Persona que disfruta con la exploración de los detalles de los sistemas programables y cómo aprovechar sus posibilidades; a diferencia de la mayoría de los usuarios, que prefieren aprender sólo lo imprescindible.

Hardware: Conjunto de componentes que integran la parte física de una computadora (teclado, mouse, monitor, etc).

HR: Human Recognition (Reconocimiento Humano).

IBC: International Biometric Group, Empresa líder de consultoría y servicios en el campo de la tecnología biométrica.

Identidad: Es el conjunto de características o circunstancias que hacen que alguien o algo sea reconocido sin posibilidad de confusión con otro.

Identificar: Reconocer que una persona o cosa es la misma que se supone o se busca.

Información: Es un conjunto de datos que constituyen un mensaje sobre un determinado fenómeno.

Integridad: Se refiere al control sobre los datos a fin de asegurar que el contenido de la información no se modifique sin la debida autorización y que durante la transmisión la secuencia de los datos se mantenga.

Interfaz: Conexión física y funcional entre dos aparatos o sistemas independientes.

ISO: International Organization for Standardization. Es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

IT: Tecnología de la Información.

Lenguaje de Programación: Lenguaje que se utiliza para escribir programas de computadora.

MAC: Message Authentication Code. Es un código que se genera a partir de un mensaje de longitud arbitraria y de una clave secreta compartida entre remitente y destinatario, y que sirve para autenticar el mensaje.

Método Científico: Es un proceso destinado a explicar fenómenos, establecer relaciones entre los hechos y enunciar leyes que expliquen los fenómenos físicos del mundo y permitan obtener, con estos conocimientos, aplicaciones útiles al hombre.

Minucias: El término hace referencia a ciertas características de las huellas dactilares (arcos, bucles, etc.) que hacen posible la identificación de individuos.

NBCT: United States National Biometric Test Center. Este centro fue creado por el Consorcio Biométrico del Departamento de Defensa Americano a finales de 1997. Su principal objetivo es llevar más lejos los esfuerzos en estandarización biométrica relacionados por el gobierno de los Estados Unidos, generando procedimientos estándares de prueba o validación y midiendo objetivamente el rendimiento de los sistemas biométricos implementados existentes en el mercado.

NCITS: National Committee for Information Technology Standars. Comité cuyo objetivo es generar estándares consensuados, de forma voluntaria, teniendo en cuenta el mercado, en las áreas de multimedia, intercomunicación entre sistemas de información y computadoras, medios de almacenamiento, bases de datos, seguridad y lenguajes de programación.

NIST: National Institute of Standars and Technology**,** fundada en 1901, es una agencia federal no regulatoria dentro del departamento de Comercio de los Estados Unidos que desarrolla y promueve tecnología y estándares.

NOM: Norma Oficial Mexicana. Una NOM es la regulación técnica de observancia obligatoria expedida por las dependencias competentes, conforme a las finalidades establecidas en el artículo 40, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como, aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado y las que se refieran a su cumplimiento o aplicación.

Patrón (template): Es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

PIN: Personal Identification Number. Es una contraseña o clave numérica que se utiliza para acceder a cajeros automáticos y servicios de telefonía entre otros.

Red de Computadoras: Conjunto de dos o más equipos interconectados entre sí a fin de llevar a cabo el intercambio de información de manera eficiente y confiable.

RFID: Radio Frequency Identification, es un sistema de almacenamiento y recuperación de datos. El propósito fundamental de esta tecnología es transmitir la identidad de un objeto mediante ondas de radio.

Ruido: Perturbación eléctrica que interfiere sobre las señales transmitidas o procesadas.

Señal: Es la variación de una corriente eléctrica u otra magnitud física que se utiliza para transmitir información.

Seguridad: Confianza, tranquilidad, certidumbre procedente de la idea de que no hay peligro que temer.

Seguridad Informática: Nombre genérico dado a una colección de herramientas diseñadas para la protección de datos, sistemas de cómputo y detener a los perpetradores.

Sensor: Dispositivo que detecta una acción externa, temperatura, presión, entre otras, y la transmite adecuadamente.

Sistema: Es una combinación de componentes que actúan conjuntamente y cumplen un objetivo determinado.

Sistema Biométrico: Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas.

Smartcard: Tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.

Software: Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora.

Tecnología Biométrica: La tecnología biométrica es el desarrollo de aplicaciones que permiten llevar a cabo de manera automatizada la identificación y verificación de la identidad de los individuos.

Token: Es un dispositivo electrónico que se le da a un usuario autorizado de un servicio computarizado para facilitar el proceso de autenticación.

Transistor: Dispositivo electrónico semiconductor provisto de tres o más electrodos que sirve para rectificar y amplificar los impulsos eléctricos. De tamaño pequeño, el transistor opera con voltajes pequeños y puede admitir corrientes relativamente intensas.

Verificar: Probar que algo es verdadero o exacto.

Virus: Los virus son programas que infectan documentos o sistemas mediante la inserción o la agregación de una copia de sí mismo o mediante la reestructura de archivos completos. Los virus trabajan sin el consentimiento ni la autorización del usuario.

Vulnerabilidad: Debilidad que puede ser explotada para violar la seguridad.

WWW: World Wide Web o Red Mundial. Sistema de servidores de Internet con páginas formateadas en un lenguaje de programación llamado HTML, y que contienen enlaces a otros documentos a los que se acceden mediante hipervínculos.

APÉNDICE A

Dispositivos de Adquisición de Huella Dactilar.

En el mercado actual, existe una gran variedad de dispositivos de captura de huellas dactilares. Todos ellos obedecen a escáneres de tipo *inkless*, es decir, dispositivos que posibilitan la adquisición de las huellas sin necesidad de utilizar tinta para calcar las huellas dactilares en papel. Entre los dispositivos más utilizados podemos encontrar las pantallas táctiles (touch screen), los escáneres y las cámaras fotográficas.

A.1. Pantallas Táctiles (Touch Screen).

Actualmente existen pantallas táctiles con tecnologías distintas: capacitiva, resistiva, infrarroja, de ondas acústicas, entre otras; aunque todas funcionan con el mismo principio: la alteración de un flujo de energía en algún punto de la pantalla, causado por un dedo, pluma, etc., para medir las coordenadas del punto tocado con relación a las esquinas de la pantalla.

A.1.1. Tecnología Capacitiva.

Una pantalla táctil que funciona con base en este tipo de tecnología, consiste en una membrana de vidrio con una delgada capa metálica sobre la superficie de la pantalla. Se aplica una ligera corriente eléctrica a la pantalla, la cual se altera solamente cuando la pantalla es tocada con un dedo o bien con un objeto conductor de electricidad (véase figura A.1). Las membranas capacitivas utilizadas son resistentes a arañazos y su desempeño no se ve afectado por manchas de grasa, solventes, polvo o agua. Las principales ventajas de esta tecnología son el bajo consumo y el reducido tamaño del dispositivo sensor, que lo hace fácilmente integrable en terminales de telefonía móvil, agendas electrónicas y kioscos informativos entre otros. Aproximadamente 80% de las pantallas táctiles instaladas en el mundo utilizan este tipo de tecnología. Por otra parte, el principal inconveniente radica en la elevada sensibilidad a variaciones en el campo eléctrico; característica que los vuelve vulnerables a la contaminación electromagnética presente en el entorno de captación.

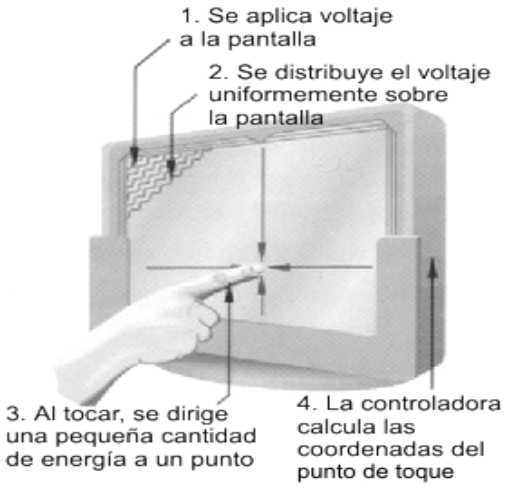


Figura A.1 Funcionamiento de una membrana capacitiva

A.1.2. Tecnología Resistiva.

Una pantalla táctil resistiva está formada por varias capas. Las más importantes son dos finas capas de material conductor entre las cuales hay una pequeña separación. Cuando algún objeto toca la superficie de la capa exterior, las dos capas conductoras entran en contacto en un punto concreto. De esta forma se produce un cambio en la corriente eléctrica que permite a un controlador calcular la posición del punto en el que se ha tocado la pantalla midiendo la resistencia. Las pantallas táctiles resistivas son por norma general más asequibles pero tienen una pérdida de aproximadamente el 25% del brillo debido a las múltiples capas necesarias. Otro inconveniente que tienen es que pueden ser dañadas por objetos afilados. Por el contrario no se ven afectadas por elementos externos como polvo o agua.

A.1.3. Ondas Acústicas.

Esta tecnología se basa en la transmisión de ondas acústicas sobre la superficie de una membrana de vidrio puesta sobre la pantalla (véase figura A.2). Se activa presionando con una pluma de punta suave o con un dedo. Cuando la pantalla es tocada, una parte de la onda es absorbida. Este cambio en las ondas de ultrasonidos permite registrar la posición en la que se ha tocado la pantalla y enviarla al controlador para que pueda procesarla. Los dispositivos que utilizan este tipo de tecnología deben encontrase en ambientes limpios pues su funcionamiento puede verse afectado por elementos externos tales como polvo, líquidos u otros contaminantes.

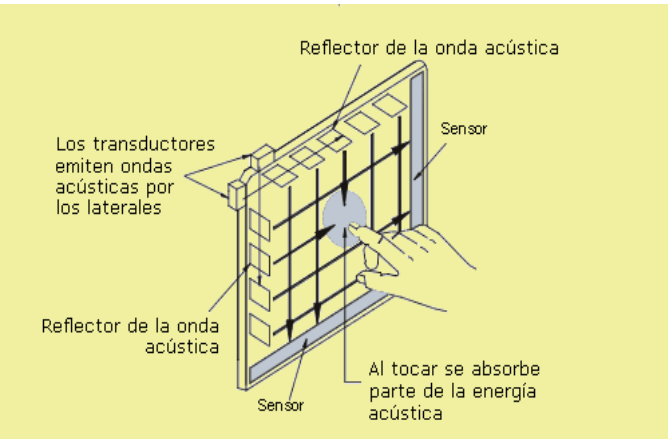


Figura A.2 Funcionamiento de una membrana por ondas acústicas.

A.1.4. Tecnología Infrarroja.

Esta tecnología está compuesta de tableros cableados y un bisel infrarrojo transparente (véase figura A.3). Al tocar la pantalla, se interrumpe el flujo de los rayos infrarrojos para determinar las coordenadas del toque. Una desventaja de esta tecnología es que puede activarse sin tocar la pantalla, por lo cual podrían registrase “toques falsos”; además cuenta con una baja resolución y requiere con un costoso bisel diseñado a la medida de la aplicación.

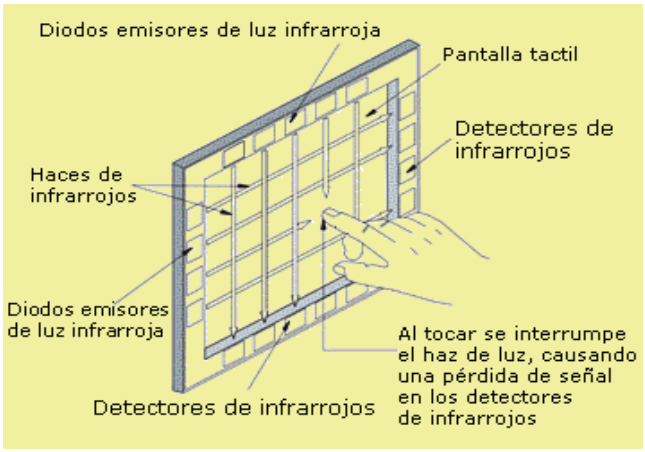


Figura A.3 Funcionamiento de una membrana por Infrarrojos.

A.2. Escáneres.

Los escáneres son periféricos diseñados para registrar caracteres escritos o gráficos facilitando su introducción en la computadora convirtiéndolos en información binaria comprensible para ésta. El funcionamiento de un escáner es similar al de una

fotocopiadora. Se coloca una imagen sobre una superficie de cristal transparente, bajo el cristal existe una lente especial que realiza un barrido de la imagen; al realizar el barrido, la información es convertida en una sucesión de información en forma de unos y ceros que se introducen en la computadora.

Una de sus principales ventajas es la velocidad de lectura e introducción de la información en el sistema informático con respecto al método tradicional de introducción manual de datos por medio del teclado, llegándose a alcanzar los 1200 caracteres por segundo.

Al iniciar la exploración de la imagen, ésta es expuesta a una fuente de luz, la cual refleja la imagen que es conducida mediante un sistema de espejos y lente hacia el CCD (Charge Coupled Device- Dispositivo Acoplado por Carga Eléctrica). Los espejos están situados en el carro de exploración, el cual es impulsado por un motor y transmite su movimiento mediante un sistema de correas (véase figura A.4).

El CCD es el componente fundamental de un escáner ya que de él depende la resolución que puede alcanzar la imagen digitalizada. La resolución se mide en ppp (puntos por pulgada). Un escáner tiene diferentes tipos de resolución. La resolución óptica es el número de puntos individuales de una imagen que es capaz de captar el CCD. Ésta es la resolución más importante porque define los límites físicos del escáner. Se expresa dando los ppp horizontales por los ppp verticales. La resolución interpolada está dada por puntos creados en la computadora, que acomoda entre los puntos captados en la resolución óptica. Estos puntos “inventados” deben sus características a los puntos ópticos que tengan al lado. Por ejemplo, la computadora puede intuir que entre un punto blanco y uno negro se encontraba uno gris, entonces lo crea y lo acomoda entre ellos. Esto aumenta mucho la resolución, pero siempre depende de la resolución óptica o real. Por ejemplo, la computadora puede intuir que entre un punto blanco y uno negro se encontraba uno gris, entonces lo crea y lo acomoda entre ellos. Esto aumenta mucho la resolución, pero siempre depende de la resolución óptica o real.

Después de pasar por el CCD, las señales eléctricas son recibidas por un Convertidor analógico -digital llamado DAC (Digital Analog Converter), que las convierte en píxeles digitales, los cuales forman nuevamente la imagen en la computadora.

En general los escáneres de huellas dactilares electrónicos aciertan entre el 95 y el 98 por ciento de las veces. Pero la exactitud varía en función del sexo, características raciales y residuos químicos en los dedos.

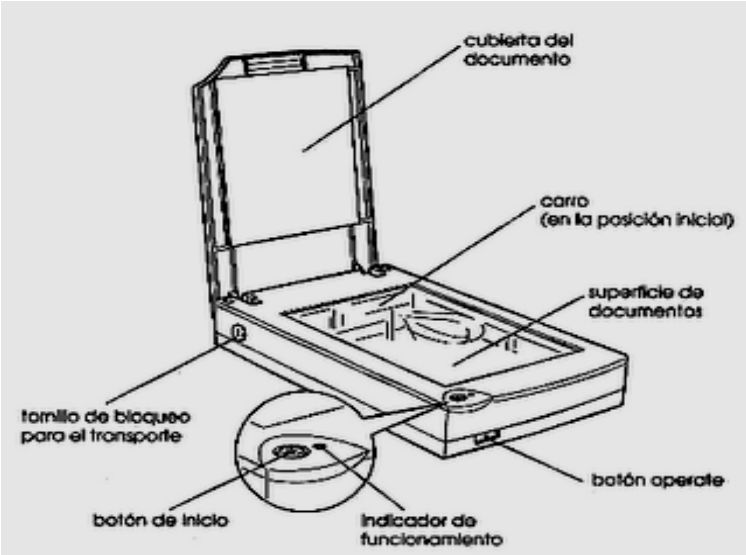


Figura A.4 Funcionamiento del escáner.

APÉNDICE B

Portada sellada de la Propuesta de Estándar

Universidad Nacional Autónoma de México

Facultad de Ingeniería

GUÍA PARA EL USO SEGURO DE TECNOLOGÍAS BIOMÉTRICAS

GUIDE FOR THE SAFETY USE OF BIOMETRIC TECHNOLOGIES

Bibliografía y Mesografía

Libros de Texto:

- BEVAN James. A Pictorical Handbook of Anatomy and Physiology. Octopus Publishing Group, London, 1994.
- CARZORLA Quevedo Miguel Ángel, et.al. Fundamentos de Inteligencia Artificial. Publicaciones de la Universidad de Alicante, España, 1999.
- GREEN J.H. Manual de Fisiología Humana. Editorial Marín, S.A., España, 1969.
- IBÁÑEZ Reséndiz Rosendo. La Huella Digital y el Derecho Mexicano. Editorial SISTA, México, 1989.
- LOVATT Evans Charles. Principios de Fisiología Humana. Editorial Aguilar, Madrid, 1995.
- MONPÍN Poblet José, et.al. Inteligencia Artificial: conceptos, técnicas y aplicaciones. Ediciones Marcambo S.A., Barcelona, 1987.
- OYSTER Clyde W. The Human Eye. Structure and Function. Sinauer Associates, Inc., Sunderland, Massachusetts, 1999.
- RAMOS Denia Ángel. Pequeño tratado de Dactiloscopia. Ediciones Gernika, México, 1992.
- TAPIADOR Mateos Mariano, et.al. Tecnologías Biométricas aplicadas a la seguridad. Editorial Alfaomega, Madrid, 2005.
- TRUJILLO Arriaga Salvador. El estudio Científico de la Dactiloscopia. Editorial Limusa, México, 1987.

Revistas.

- MARTÍNEZ García Juan Carlos. "El reinado de la Biometría". *¿Cómo ves?,* Año 9, No 104, pp. 10-14, Julio 2007.

Sitios de Internet:

- AMBI. http://www.ambi.org.mx
- Anatomía de la mano humana. http://es.wikipedia.org/wiki/Mano
- ANSI. http://www.ansi.org

- Antecedentes Históricos de la Biometría.

  http://www.monografias.com/trabajos43/biometria/biometria.shtml

- BioAPI. http://www.bioapi.org

- Biometría óptica del Iris. http://www.upc.edu.pe/html/0/0/carreras/ing-electronica/proyectos/Biometr%C3%ADa-%C3%B3ptica-de-iris.pdf

- Blog. http://es.wikipedia.org/wiki/Blog

- CBEFF.

  http://www.itl.nist.gov/div895/isis/bc/cbeff/
  http://www.homepage.ntlworld.com/avanti/nist.pdf

- Dactiloscopia.

  http://www.criminalistica.com.mx/DescargablesPDF/DactiloscopiaJMJM.pdf
  http://www.monografias.com/trabajos56/huellas-lofoscopicas/huellas-lofoscopicas4.shtml

- El iris Ocular como parámetro para la Identificación Biométrica.

  http://www.revistasic.com/revista41/pdf_41/SIC_41_agora.PDF

- Especificación de BAPI (Microsoft). http://www.iosoftware.com

- Foro. http://es.wikipedia.org/wiki/Foro_(Internet)

- Geometría de la mano.

  http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Hand%20Geometry.pdf

- HA-API.

  http://www.biometrics.org/html/standars.html
  http://www.biometrics.org/REPORTS/HAAPI20/

- Identificación Biométrica con Huellas Digitales.

  http://ciberhabitat.gob.mx/hospital/huellas/textos/identificacion.htm

- INCITS. http://www.ncits.org/

- Informática Social.

  http://www.monografias.com/trabajos14/informatica-social/informatica-social.shtml

- Introducción a la biometría.

  http://www.monografias.com/trabajos43/biometria/biometria.shtml

- ISO. http://www.iso.ch/

- NIST. http://www.nist.gov

- Puntos singulares y orientación para la clasificación de Huellas dactilares.

  http://ma1.eii.us.es/miembros/rogodi/td0708/27/pre.pdf

- Reconocimiento de Patrones.

  http://catarina.udlap.mx/u_dl_a/tales/documentos/lep/franco_g_ja/capitulo4.pdf
  http://www.gts.tsc.uvigo.es/pi/Reconocimiento.pdf
  http://iie.fing.edu.uy/ense/asign/recpat/material/sistemas_rec_patrones.pdf

- Sistemas Biométricos.

  http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm
  http://www.disa.bi.ehu.es/spanish/asignaturas/17223/Sistemas_Biometricos.pdf

- Sistema de reconocimiento de Huellas dactilares.

  http://www.depi.itchihuahua.edu.mx/electro/archivo/electro2001/mem2001/articulos/dsp3.pdf

- Tecnologías de la Información.

  http://es.wikipedia.org/wiki/Tecnolog%C3%ADa_de_la_informaci%C3%B3n

- Wiki.

  http://es.wikipedia.org/wiki/Wiki
  http://www.maestrosdelweb.com/editorial/queeswiki/

- X9. http://www.x9.org