UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

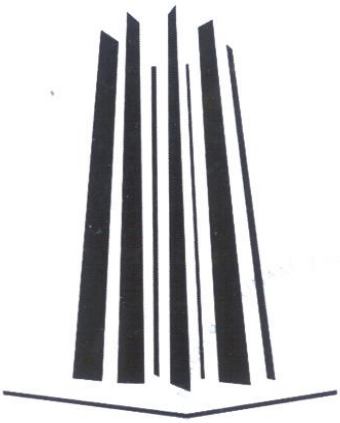
AUTENTICACIÓN BIOMÉTRICA POR EL MODO DE ANDAR

TESIS

QUE PARA OBTENER EL TÍTULO DE INGENIERO EN COMPUTACIÓN

PRESENTA:

RAMSÉS LÓPEZ GUERRERO



DIRECTOR DE TESIS:
MAT. LUIS RAMÍREZ FLORES

MÉXICO, D.F. **OCTUBRE 2009**

RECONOCIMIENTOS

Primordialmente quiero agradecer a DIOS por su apoyo y fortaleza que siempre me ha brindado y por quien si no fuera por él no podría salir adelante. Este trabajo jamás hubiera sido realizado sin su ayuda.

AGRADECIMIENTOS

A DIOS.

A mi madre Teresa Guerrero Basurto quien siempre ha sido mi orgullo y quien me brindó los cimientos sólidos para ser una persona de bien.

A mi padre Víctor López Zúñiga quien siempre me ha apoyado en todos los aspectos.

A mi amiga a quien aprecio y quiero mucho, la Lic. Claudia Tatiana Chávez Castro quien siempre me ha brindado su apoyo y que sin el cual este sueño hubiera tardado más tiempo.

A mi amigo, el MBA Adalberto Francisco García Espinosa a quien aprecio y admiro, y al cual le agradezco totalmente su apoyo brindado en el transcurso de este trabajo de tesis.

DEDICATORIA

A DIOS.

Por último, pero no por ello menos importante a mi mejor amiga y compañera Maureen Guadalupe Nava Morales a quien quiero, aprecio y agradezco mucho su cariño, consejo y apoyo brindado.

ÍNDICE DEL CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Existen muy pocas investigaciones sobre este tema en habla española y más aun en México, es por esto que desafortunadamente para las personas que únicamente conocen el español, la mayoría de estos textos están en otros lenguajes, o bien, las traducciones que se hacen de esos textos suelen modificar el significado o la idea que el autor deseaba expresar; la mayoría de las investigaciones son de investigadores de Estados Unidos, Alemania y la India y es por eso que algunos de los términos se tuvieron que dejar como nativos de esas lenguas, por el hecho de que no existe una traducción apropiada al español, o porque la traducción restaba significado al concepto.

No hay duda que las aplicaciones de seguridad juegan un papel importante en el futuro y que la tecnología biométrica es un importante componente en la seguridad informática. Aunque el 100% de la protección nunca puede ser lograda, es importante determinar la correcta tecnología biométrica para cada aplicación en particular. Esta tesis es una contribución al desarrollo de una nueva generación de comodidad al usuario y facilidad para operar los sistemas de autenticación biométricos, el cual abre un nuevo campo a posibles aplicaciones.

Muchas investigaciones actuales tienen como *único objetivo* el implementar sistemas o algoritmos de reconocimiento de patrones para la manera de caminar de las personas, sin preocuparse de que muchas veces el entorno en que se lleva a cabo, no siempre es el ideal; es decir, muchas veces las soluciones no pueden ser llevadas a cabo por el simple hecho de implementar el sistema o el algoritmo; esto porque no es posible esperar que un usuario camine por ejemplo siempre por el mismo lugar, si usará los mismos zapatos, si está cansado o simplemente porque trae una bolsa en la mano, entonces no puede ser esperado que ese mismo algoritmo funcione en todo momento y en todo escenario o mas particular aún si ese algoritmo funcione únicamente como un método de identificación y no como un método de autenticación.

Entonces este es mi punto de partida, este trabajo de investigación comprenderá un estudio exhaustivo de la biométrica por la manera de caminar de las personas **y se espera demostrar si la biometría por la manera de caminar de las personas puede ser implementada como un método de autenticación.** Para ello se estudian dos vertientes: si la manera de caminar de las personas puede ser implementada como un método de autenticación y la segunda es, en

que escenarios pude ser llevada a cabo ésta; por tal motivo se propone como objetivo hacer al lector una mente analista para que pueda discernir el momento en que esta tecnología pudiera ser ideal para ser utilizada como una forma de autenticación si es que este pudiera ser el caso.

Hago mención del objetivo de cada uno de los capítulos que se mostrarán en esta investigación con el propósito de indicar al lector lo que espera encontrar al terminar de leer cada capítulo.

El capítulo I de conceptos básicos cita las necesidades de evaluar los compromisos de seguridad que se encuentran en todo centro de cómputo, que en nuestro estudio será el sistema de autenticación biométrico por la manera de caminar. Cito un estudio completo de lo que debemos entender como seguridad, que proteger, en contra de que proteger y cómo deben ser protegidos nuestros activos teniendo en cuenta siempre un pre-análisis de valoración de amenazas, riesgos y contramedidas para tener un balance aceptable en la elevación de los costos y la complejidad de hacer a un sistema seguro y las posibles intrusiones de un ataque o amenaza.

El estudio trata de abarcar todos los escenarios posibles; tanto los particulares como la autenticación en un solo lector biométrico, como los escenarios donde la autenticación sea remota, y por tanto más compleja, por ejemplo donde la base de datos de los modelos para autenticación se encuentren en una base de datos centralizada.

Una vez que se termine de leer el capítulo I, se comprenderá totalmente que nuestro sistema de autenticación biométrico, debe completamente verificar la identidad de alguna persona para que se garantice que ella es quien ella dice ser; y por tanto, se cumpla con el objetivo del servicio de autenticación.

El siguiente objetivo en nuestro trabajo sería elegir qué tipo de autenticación sería el más adecuado para nuestro sistema de autenticación por la manera de caminar de las personas.

Antes que nada el capítulo II explica a detalle el funcionamiento del proceso de autenticación, explicando cada una de sus etapas en el flujo del proceso de autenticación y así mismo explica minuciosamente muchas de las vulnerabilidades que se pueden

encontrar al momento de implementar cualquiera de los tipos de autenticación existentes.

El propósito de esto, es introducir claramente al lector para que analice escrupulosamente cualquier escenario posible donde la autenticación pudiera estar presente con el fin de que él mismo evalúe cada escenario donde sea encontrado dicho servicio de seguridad y de esta manera comprenda de manera fundamental y con un criterio analítico el análisis al siguiente capítulo denominado BIOMETRIA.

Entonces; el capítulo II tiene como objetivo entender los tres métodos generales de autenticación:

1. *hombre-a-hombre*
2. *hombre-a-maquina*
3. *máquina-a-máquina*

Y detalladamente todos los tipos de autenticación existentes:

1. *Alguna cosa que se conoce.*
2. *Alguna cosa que se tiene.*
3. *Alguna cosa que se es.*
4. *Algo basado en la ubicación*

Así mismo se explica que dependiendo del nivel de seguridad deseado en circunstancias particulares se puede adecuar al sistema con esquemas del tipo híbridos o multi-factores.

El capítulo III tiene como objetivo explicar detalladamente a la biometría como el proceso de autenticación elegido para nuestro sistema de autenticación por la manera de caminar de las personas.

Se explicará el detalle de cada una de las fases en que consiste un sistema biométrico:

- Registro
- Identificación
- Autenticación

Al terminar de leer dicho capítulo, el lector deberá comprender los siguientes puntos para nuestro trabajo de tesis:

- El flujo completo del proceso de autenticación biométrico.
- Los problemas que existen o se puedan presentar al analizar la implementación del sistema de autenticación biométrico.
- Entender las características generales de la topología biométrica incluyendo qué tipo de aplicaciones son utilizadas para la biometría fisiológica y cuales son utilizadas para la biometría conductual.
- Diferencias entre identificación y autenticación en un sistema biométrico.

Así mismo al momento de analizar el sistema de autenticación biométrico propuesto es fundamental e indispensable analizar su funcionamiento de acuerdo a todos y cada uno de los siguientes puntos:

- Exactitud.
- Precisión.
- Velocidad computacional.
- Coste.
- Facilidad de uso.
- Facilidad de desarrollo.
- Seguridad.
- Integridad y
- Privacidad.

El objetivo crucial de los primeros tres capítulos es dar al lector las bases analíticas y necesarias para entender un proceso de autenticación biométrico, el cual hasta este punto el lector debería de ser capaz para comprender todo aquello que engloba a un sistema de autenticación biométrico y por tal, tener el preámbulo para empezar a estudiar a la manera de caminar de las personas como un sistema de autenticación biométrico.

Se puede comenzar el cuarto capítulo con la siguiente cita bíblica, en Segunda de Samuel:

"18:24 Y David estaba sentado entre las dos puertas; y el atalaya había ido al terrado sobre la puerta en el muro, y alzando sus ojos, miró, y vio a uno que corría solo.
18:25 El atalaya dio luego voces, y lo hizo saber al rey. Y el rey dijo: Si viene solo, buenas nuevas trae. En tanto que él venía acercándose,
18:26 vio el atalaya a otro que corría; y dio voces el atalaya al portero, diciendo: He aquí otro hombre que corre solo. Y el rey dijo: Este también es mensajero.

18:27 Y el atalaya volvió a decir: Me parece el correr del primero como el correr de Ahimaas hijo de Sadoc. Y respondió el rey: Ese es hombre de bien, y viene con buenas nuevas.”

¿Por qué? si este tema ha sido tan antiguo como es citado en la biblia, ¿por qué en la actualidad apenas se encuentra bajo estudio y no existen implementaciones industriales como un modo de autenticación biométrico? El capítulo IV es el capítulo central de esta investigación y se pretende explicar uno de los métodos más nuevos que existen en la actualidad referente a sistemas biométricos. El estudio se basa en tres puntos clave:

- El caminar humano como un movimiento natural.
- Diferentes métodos y maneras de medir y obtener el reconocimiento humano.
- La manera de caminar como un modo de identificación.

Así mismo explicaré a detalle las cualidades positivas y negativas con las que podemos enfrentarnos al momento de analizar e implementar la autenticación biométrica por la manera de caminar de las personas.

El Principio de la Protección Adecuada.- Los componentes de un sistema de cómputo deben ser protegidos solamente hasta que ellos pierdan su valor.

"Segundo Principio de la Seguridad Informática"

I CONCEPTOS BÁSICOS

1.1) SEGURIDAD INFORMÁTICA

Dada la complejidad que representa el estudio y el análisis de la seguridad informática, es necesario definir ciertos conceptos y elementos que intervienen en ella.

Se entenderá como un ***sistema de cómputo*** al conjunto formado por el hardware, software, medios de almacenamiento, datos ó información y las personas involucradas en éste.

Se entenderá como un ***compromiso de seguridad*** a cualquier forma posible de pérdida o daño en un sistema de cómputo.

El término ***seguridad*** será usado en el sentido de minimizar las vulnerabilidades de los activos y los recursos [O´Gorman04].

Una ***vulnerabilidad*** será cualquier debilidad que pueda explotarse para causar pérdida o daño a un sistema.

Un **activo** será cualquier cosa con valor; donde los principales activos o recursos que hay que proteger en un sistema de cómputo son: ***hardware, software*** y ***datos.***

Entonces una ***amenaza*** será cualquier circunstancia con el potencial suficiente para causar pérdida o daño al sistema.

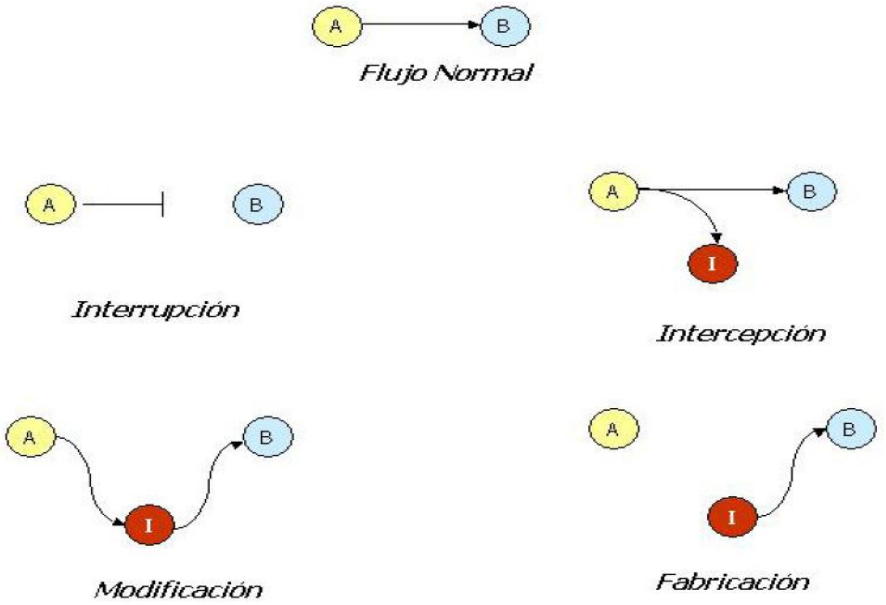


*Figura 1.- Flujo normal y amenazas a los sistemas de cómputo. La parte **A** representa a la fuente, al emisor o al origen de los datos, y la parte **B** representa al receptor o al destino. Tanto A, como B pueden ser personas, procesos, dispositivos, computadoras y en la parte literaria se les conoce también como entidades o principales (Alice & Bob)*

Existen cuatro tipos de amenazas que explotan las vulnerabilidades de los sistemas (Ver Figura 1) [Pfleeger96]:

- ***Interrupción***.- Es la pérdida, inutilización o no disponibilidad de un activo en un sistema. Como puede ser, la destrucción de un dispositivo de hardware, el borrado de un programa, el borrado de datos o de archivos, etc.
- ***Intercepción***.- Se refiere a que una parte no autorizada ha obtenido acceso a un activo. Algunos ejemplos pueden ser; la copia ilícita de un programa, la intervención en las líneas telefónicas, la escucha de un enlace de red, etc.
- ***Modificación***.- Si una parte no autorizada, además de acceder a un activo cambia su contenido, la amenaza es denominada *modificación*; como por ejemplo, el cambio de ciertos valores a una base de datos, la alteración de un programa para que ejecute un cálculo adicional, la modificación de ciertos datos que sean enviados electrónicamente, etc.
- ***Fabricación***.- Éste consiste en que una parte no autorizada crea ciertos datos sobre un sistema de cómputo. El intruso podría insertar información espuria a un sistema de comunicación de red o el agregado de registros a una base de datos.

1.2) VULNERABILIDADES

Las amenazas pueden clasificarse como:

- **Amenazas Accidentales.-** Son aquellas que existen sin ninguna intención premeditada; como pueden ser el mal funcionamiento del sistema, errores operacionales, errores en software, etc.
- **Amenazas Intencionales.-** Son aquellas que si son llevadas a cabo, pueden convertirse en un ataque. Por ejemplo, el fisgoneo de una red mediante alguna herramienta de monitoreo con el fin de irrumpir al sistema.
- **Amenazas Pasivas.-** Son aquellas, que si son llevadas a cabo, no resultarían en alguna modificación a la información contenida en el sistema; inclusive ni la operación ni el estado del sistema serían alterados. Podemos citar por ejemplo la lectura ilícita de archivos confidenciales.
- **Amenazas Activas.-** Es la alteración de la información contenida en el sistema o cambios al estado o a la operación del sistema. Un ejemplo puede ser la modificación de las tablas de encaminamiento (routing table) de un sistema por un usuario no autorizado.

En la figura 2 se muestra como pueden afectar dichas amenazas a los activos o recursos en un sistema de cómputo.

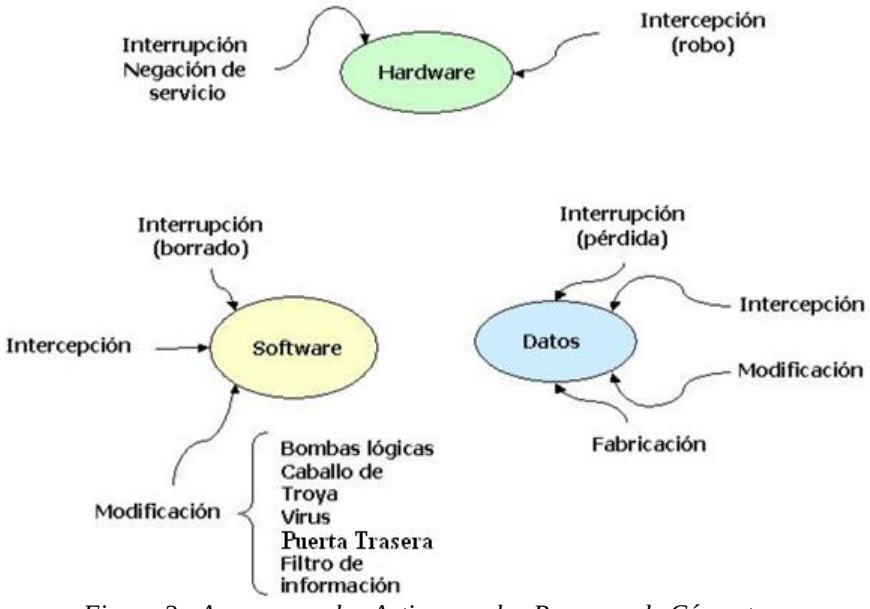


Figura 2.- Amenazas a los Activos y a los Recursos de Cómputo

1.2.1) Amenazas al Hardware

La visibilidad de los dispositivos físicos, los hace un punto de ataque más simple.

Las personas han tirado sus alimentos sobre las computadoras y sus dispositivos; aparte han sido quemadas, mojadas, electrocutadas con alteraciones de voltaje o relámpagos, pateadas, golpeadas, sacudidas, aventadas y perforadas.

También los animales han puesto su granito de arena; perros, gatos, ratones, pericos, etc.… han llegado a destruir los cables, ya sea por mordiscos, picotazos, jalones, etc.; incluso las partículas de polvo (en especial las cenizas de cigarro) llegan a perjudicar las partes electro-mecánicas de los dispositivos.

Este tipo de actos los podemos catalogar como amenazas accidentales.

Un ataque más serio podría ser intencionado, queriendo hacer daño a un sistema de cómputo…

Disparos con armas de fuego, puñaladas, bombas, fuego, incluso avionazos han destruido cuartos enteros con equipos de cómputo. Ordinarias llaves, plumas y destornilladores han servido para hacer cortocircuitos a tarjetas y a otros componentes de las máquinas. El robo no puede faltar.

Los ataques del hombre hacia las máquinas parecen no tener fin. El robo y la destrucción han sido los ataques fundamentales para limitar la disponibilidad de los equipos de cómputo. Los administradores de los centros de cómputo han instalado sistemas de seguridad para protegerlos; sin embargo la gran diversidad de microcomputadoras en oficinas trae consigo la inversión de varios miles de dólares para el aseguramiento de los equipos. Debido a las grandes sumas de dinero, muchas veces no es posible obtener un nivel de aseguramiento adecuado (en muchas ocasiones es nulo).

La seguridad física puede ser ampliamente cubierta con guardias de seguridad y/o cerraduras.

1.2.2) Amenazas al Software

Es más fácil detectar una lesión física en un equipo de cómputo que encontrar el borrado de una línea de código en un programa. Además si el cambio realizado no altera las funciones principales del programa, no sería nada fácil detectar una modificación al software, mucho menos se podría determinar la dimensión de un cambio.

Al hablar del software nos referimos al sistema operativo, utilidades y aplicaciones. Cada uno de éstos puede ser destruido maliciosamente, modificado, borrado o mal instalado.

Borrado de Software.

Probablemente todas las personas que manipulan computadoras han accidentalmente borrado archivos.

Modificación de Software

Un ataque puede causar modificación al software, causando fallas durante su ejecución o realizando tareas malintencionadas.

Cambiando un bit o dos, un programa corriendo normalmente puede hacerlo inutilizable.

Ejemplos de éstos pueden ser:

- Caballos de Troya
- Virus
- Puertas Traseras
- Bombas Lógicas
- Filtros de Información

Robo de Software

Este ataque incluye copias no autorizadas de software. Los autores de software y distribuidores tienen derecho a una compensación por el uso de sus productos, como lo son los músicos o los autores de libros. Lamentablemente hoy en día las copias no autorizadas no han sido detenidas satisfactoriamente.

1.2.3) Amenazas a los Datos

La seguridad en Hardware es usualmente un tema de un pequeño grupo de profesionistas en informática. La seguridad en software es un problema más grande, se extiende a los programadores y analistas quienes crean o modifican los programas.

Los programas son escritos en un lenguaje que sólo lo conocen un selecto grupo de profesionistas en cómputo; así que la revelación de una parte del código de un programa no tendría sentido al público en general. Los datos por el contrario, pueden ser fácilmente interpretados por casi cualquier persona; entonces, el ataque a los datos es un más grave y serio problema público que los ataques al hardware y al software.

Los datos no tienen esencialmente un valor intrínseco. Por esta razón *es muy difícil medir el valor de un dato.* Sin embargo los datos tienen un costo, quizás por el costo de su reconstrucción, o por volver a desarrollar el dato.

Un dato modificado incorrectamente puede costar vidas humanas. Por ejemplo, un error en el tiempo en que se deben aplicar las dosis de insulina a un paciente con diabetes, pueden ocasionarle una sobredosis y posiblemente la muerte.

El hardware y el software tienen en muchas ocasiones un gran tiempo de vida en comparación a los datos. El valor del dato puede ser alto, pero en algunos casos los datos son de interés solamente por un corto periodo de tiempo. Consideremos el siguiente ejemplo.

Imaginemos un ataque decisivo en la segunda guerra mundial entre Japón y los EUA, en el cual iba a haber una invasión de parte de Estados Unidos. Para ello se necesitaban difundir instrucciones muy precisas a ciertas tropas en el territorio enemigo por medio de un código, pero tenían que difundirlas en menos de 24 horas.

El esquema de protección adecuado debería de tomar a un intruso más de 24 horas romper el código, pues después de ese tiempo ya no habría necesidad para tener confidencialidad en los datos.

1.3) ATAQUES

Un ***ataque*** entonces lo podemos definir, como cualquier acción que explote alguna vulnerabilidad. A esta entidad se le puede conocer como ***atacante, intruso, enemigo, cracker, hacker,*** incluso si hablamos de una persona o un grupo de personas también se les puede denominar ***delincuente ó criminal informático o computacional***.

Hay diversas maneras de catalogar los ataques, una de ellas es por su origen: Internos y Externos.

1.3.1) Ataques Internos (Insider Attacks)

Éstos ocurren cuando los usuarios legítimos de un sistema se comportan de manera anormal o no autorizada. Muchos crímenes computacionales son cometidos así. Algunas de las medidas de protección pueden ser:

- Cuidadosa elección del personal.
- Examinación de hardware, software, políticas de seguridad y configuraciones del sistema para la certeza de su correcta operación.
- Auditorías; para incrementar la probabilidad de detectar ataques.

1.3.2) Ataques Externos (Outsider Attacks)

Pueden usar técnicas como:

- Escucha del cable (wire tapping); ya sea, activa o pasiva.
- Interceptación de emisiones.
- Enmascaramiento
- Evitar los mecanismos de autenticación y/o control de acceso

1.3.3) Algunos Tipos de Ataques

1.3.3.1) Enmascaramiento (Masquerade)

Es cuando una entidad pretende ser una entidad diferente. Usualmente es usada con algunas otras formas de ataques activos; especialmente replicas y modificaciones de mensajes. Por ejemplo, cuando en una comunicación se hace un envío de credenciales para

la autenticación de un usuario y un atacante las graba, éste puede repetirlas después, para autenticarse obteniendo los privilegios del usuario atacado.

1.3.3.2) Replica (Replay)

Ocurre cuando un mensaje, o parte de un mensaje, es repetido para producir un efecto no autorizado. Por ejemplo, un mensaje grabado conteniendo información de autenticación puede ser repetido por otra entidad para autenticarse ella misma.

1.3.3.3) Modificación de Mensajes (Modification of Messages)

Ocurre cuando una transferencia de datos es alterada sin detección y da como resultado un efecto no autorizado; por ejemplo, cuando un mensaje podría ser cambiado de: Permite a "*Juan Hernández*" leer el archivo confidencial de "Cuentas" a: Permite a "*Pedro Hernández*" leer el archivo confidencial de "Cuentas".

1.3.3.4) Denegación de Servicio (Denial of Service)

Ocurre cuando una entidad falla al momento de ejecutar su propia función, o actúa en un camino que impide a otras entidades ejecuten sus propias funciones. Aunque no siempre es posible prevenir una condición de denegación de servicio, los servicios de seguridad (que serán explicados más adelante) se pueden emplear para detectar una denegación de servicio y con ello tomar medidas correctivas.

Esta detección puede no ser capaz de determinar si la condición es resultado de un ataque o de una condición accidental. Ataques intencionales en la denegación de servicio pueden ser el borrado de tráfico o la generación de tráfico extra; y posibles causas accidentales pueden ser tormentas o terremotos [X.81096].

Esta identificación y las medidas correctivas aparte de implicar el uso de servicios de seguridad, también pueden implicar el uso de servicios de no seguridad como por ejemplo; el desvío de tráfico por otros enlaces, pasar a medios de almacenamiento de reserva o arrancar los procesadores de reserva.

Muchos tipos de servicios están sujetos a ataques por servicio, y los mecanismos que se emplean para prevenirlos varían según el tipo de aplicación que se va a proteger. Por eso es imposible clasificar de forma general los mecanismos de protección en contra de la denegación de servicio.

1.3.3.5) Puerta Trasera (Trapdoor)

Cuando una entidad de un sistema es alterada para permitir a un atacante producir un no autorizado efecto sobre un comando o un predeterminado evento o secuencia de eventos, el resultado es denominado *puerta trasera*. Por ejemplo, un programa podría validar la clave de ciertos usuarios, pero podría ser modificado para que aparte de su funcionamiento normal, dejara un punto de entrada secreto, para que también se valide la clave de un atacante.

1.3.3.6) Caballo de Troya (Trojan Horse)

Es un programa introducido dentro de un sistema que aparte de realizar sus funciones permitidas, realiza funciones no autorizadas. Por ejemplo, en una comunicación que además del flujo normal de transmisión copiara mensajes a un canal no autorizado sería denominado *Caballo de Troya.*

1.3.3.7) Virus

Es un programa o fragmento de código que puede propagar su infección de un programa a otro o de una computadora a otra. Para que un virus pueda ser activado el software debe ser ejecutado primero.

1.3.3.8) Filtración de la Información (Information Leaks)

Es cuando en un programa, se filtra la información para que sea accesible a una no deseada persona o programa.

1.3.3.9) Bomba Lógica (Logic Bomb)

Es una pieza de código intencionalmente colocada dentro de un sistema para que ejecute ciertas funciones maliciosas cuando condiciones específicas sean reunidas. Por ejemplo un programador

inconforme por un despido injustificado podría insertar una bomba lógica en el sistema para que después de 10 días que él ya no trabajaba en la empresa, borrara la base de datos de la nómina 5 horas antes del corte de pago.

1.3.3.10) Ataque Salami (Salami Attack)

Son una serie de ataques que toman lugar cuando pequeñas, casi inmateriales cantidades de activos, son sistemáticamente adquiridas desde diversos orígenes. Son cantidades tan pequeñas que, por lo general existen debajo del umbral de percepción y por lo tanto, difícilmente detectadas.

Imagine a un criminal que podría escribir un programa el cual reduzca el rendimiento personal de los intereses mensuales de cada uno de los clientes de un banco a 0.00001% y que en cada una de estas transacciones por cliente, el dinero pasara a la cuenta del criminal.

El resultado obtenido sería la acumulación de activos de tal manera que las víctimas, no se percataran de la desaparición de sus activos. Menos probable sería que un cliente pudiera alertar al banco por un ínfimo error en sus cuentas.

1.4) VALORACIÓN DE LAS AMENAZAS, RIESGOS Y CONTRAMEDIDAS

La seguridad generalmente eleva los costos y la complejidad de un sistema. Es por esto, que antes de implementar seguridad en un sistema, es necesario identificar sus amenazas. Una vez identificadas, se sabrá en contra de que se va a proteger.

Un sistema es vulnerable en muchos aspectos, pero solamente en algunos es explotable, pues el resultado del ataque tiene que justificar el riesgo y el esfuerzo de la intrusión. Algunas de las características que deben ser llevadas a cabo para la valoración de amenazas son:

- Identificación de vulnerabilidades en el sistema
- Análisis de probabilidad de las amenazas que pudieran explotar alguna vulnerabilidad

- Evaluación de las consecuencias si cada una de las amenazas fueran exitosamente llevadas a cabo
- Estimar el costo de cada uno de los ataques
- Calcular el costo de las posibles contramedidas
- Elegir los mecanismos de seguridad que sean justificados (posiblemente usando el análisis costo-beneficio)

Es comprensible entender ahora que el objetivo de la seguridad no es hacer a un sistema perfectamente seguro, pues no es posible hacerlo ni físicamente, ni técnicamente. El objetivo por lo tanto, es hacer el costo de un ataque lo suficientemente alto para reducir el riesgo a niveles aceptables.

1.5) POLÍTICA DE SEGURIDAD

Como se ha visto hasta ahora, el campo de la seguridad es tanto complejo como inalcanzable, pues un análisis completo produciría una desalentadora variedad en detalles. La política de seguridad o normativa de seguridad es entonces quien debe enfocarse en los aspectos más importantes que debieran recibir atención.

En términos generales, es quien dice que es y que no es permitido en el campo de la seguridad. Usualmente no es específica; más bien, sugiere que es de suma importancia sin precisar como el resultado debe ser obtenido.

La política de seguridad puede especificar cierto tipo de acciones; como la generación de un informe de alarma de seguridad, el registro de un evento en un registro de auditoría, el incremento del contador de umbrales, incluso ignorar el evento o cualquier combinación de las anteriores [X.73692].

Como en un principio una política de seguridad es definida de manera general, no es del todo clara. El mejor camino para establecer políticas más claras es agregar mayor detalle a la política; para esto un estudio por fases sobre el área de inquietud proporcionaría la información necesaria para agregar mayor detalle y con esto, el proceso de refinamiento produciría una política general en términos más precisos y más claros.

En su forma más simple podemos definir a la política de seguridad como un conjunto de criterios para la provisión de los servicios de seguridad [X.84101].

1.6) SERVICIOS Y MECANISMOS DE SEGURIDAD

Los objetivos de las políticas de seguridad deben ser logrados mediante los **servicios de seguridad,** los cuales deben ser implementados mediante **mecanismos de seguridad.** Estos mecanismos que son determinados por las amenazas previstas y el valor de los recursos que hay que proteger [X.81096], consisten en alguna funcionalidad específica para algún servicio de seguridad específico.

Para ello, las **reglas de seguridad** son la información local que nos ayuda, dados los servicios de seguridad seleccionados, para especificar los mecanismos de seguridad subyacentes que se deben de emplear, incluyendo todos los parámetros necesarios para el buen funcionamiento del mecanismo [X.80295].

1.6.1) Arquitectura de Seguridad OSI (ISO 7498-2 ó ITU-T X.800)

La OSI (Open Systems Interconnection) se encarga de la interconexión de sistemas de cómputo heterogéneos para que la comunicación entre procesos de aplicación pueda ser lograda.

En varias ocasiones, controles de seguridad deben ser establecidos en orden para proteger el intercambio de información entre los procesos de aplicación. El estándar ISO 7498-2 ó la Recomendación ITU-T X.800 de contenido idéntico, cubren la seguridad en la comunicación entre sistemas abiertos.

Los objetivos de esta arquitectura proporcionan una descripción general de los servicios y mecanismos relacionados a la seguridad y define donde pueden ser proveídos dentro de las capas OSI.
En la práctica los servicios deben de ser invocados en sus apropiadas capas y en apropiadas combinaciones, usualmente con *servicios y mecanismos no OSI* para satisfacer la política de seguridad y/o los requerimientos del usuario.

1.6.1.1) Servicios de Seguridad

Un servicio de seguridad es una característica que debe tener un sistema para satisfacer una política de seguridad. En otras palabras, es quien *identifica* lo que es requerido.

1.6.1.1.1) Autenticación

Estrictamente existen dos tipos de autenticación: La autenticación en una comunicación entre un par de entidades y la autenticación del origen de datos.[1]

Autenticación de un par de entidades.- *Este servicio es proveído para usarse en el establecimiento de, o en el tiempo durante el cual, la fase de transferencia de datos de una conexión, confirma las identidades de una o más de las entidades conectadas a una o más de las otras entidades.*

De acuerdo a la naturaleza de los elementos en que se basa su implementación podemos clasificarla en cuatro tipos:

- **Alguna cosa que se conoce**
- **Alguna cosa que se tiene**
- **Alguna cosa que se es**
- **Algo que determina su posición en la Tierra**

Autenticación del origen de datos.- *Provee la corroboración del origen de una unidad de datos.*

Es la certeza de que los datos hayan salido de donde se supone debieron haber salido y no exista la posibilidad de haber suplantado al origen.

[1] Otros tipos de autenticación que no son explicados a detalle en 7498-2 ó X.800 son:

Directa.- Cuando sólo intervienen las partes interesadas que se van a autenticar.
Indirecta.- Cuando interviene una tercera parte confiable que actúa como autoridad o juez quien avala la identidad de las partes.
Unidireccional.- Cuando basta que una de las partes se autentique ante la otra y no es necesario que la otra se autentique, a su vez, ante la primera.
Bidireccional.- Cuando se requiere que ambas partes se autentiquen entre sí.

1.6.1.1.2) Control de Acceso

Este servicio protege a los activos del sistema contra los accesos y usos no autorizados. Existen un gran número de técnicas propias y tipos de control de acceso como los basados en funciones (RBAC) [X.80503], inclusive modelos específicos para lograr los objetivos del control de acceso, tales como los de Bell y LaPadula y Clark y Wilson, entre otros.

Este servicio está cercanamente relacionado al de autenticación, ya que un usuario debe generalmente ser autenticado antes de tener acceso a los activos del sistema. Por esta razón, su estudio detallado se integra con el de autenticación, en algunas de sus partes.

1.6.1.1.3) Confidencialidad de los Datos

Este servicio de seguridad consiste en garantizar que los datos no sean divulgados sin autorización [X.80503] a personas, entidades o procesos [X.81496]. En algunos contextos este servicio se conoce también como **privacidad.**

El estándar y la recomendación identifican los siguientes tipos de servicios de confidencialidad.

Confidencialidad Orientada a una Conexión.- *Provee la confidencialidad de todos los datos de usuario sobre una conexión [X.81496]*.

Confidencialidad Orientada a una no Conexión.- *Provee la confidencialidad de todos los datos de usuario sobre una comunicación sin conexión.*

Confidencialidad Selectiva de Campo.- *Provee la confidencialidad en ciertos campos seleccionados entre los datos del usuario sobre una conexión o sobre una simple unidad de datos en una comunicación sin conexión.*

Confidencialidad del Flujo de Tráfico.- *Este servicio provee la protección de la información que podría derivarse de la observación del flujo de tráfico.*

1.6.1.1.4) Integridad de los Datos

Este servicio protege a los activos del sistema contra todo tipo de acción que atente contra la integridad de los activos que no esté autorizada [X.81596]; como pueden ser las modificaciones, las alteraciones, borrados, inserciones, etc.

Estrictamente hablando, la integridad como tal no se puede garantizar, lo que sí se puede garantizar, es que si la información sufre algún tipo de alteración ésta pueda ser detectada (verificación de la integridad).

Integridad de la Conexión con Recuperación- *Provee la integridad de todos los datos de usuario sobre una conexión con intento de recuperación.*

Integridad de la Conexión sin Recuperación.- *Provee la integridad de todos los datos de usuario sobre una conexión sin intento de recuperación.*

Integridad de la Conexión con Campos Seleccionados.- *Provee la integridad de campos elegidos entre los datos de usuario en una unidad de datos transferidos sobre una conexión.*

Integridad Orientada a la no Conexión.- *Determina si una simple unidad de datos recibida ha sido modificada en una comunicación orientada a la no conexión.*

Integridad Orientada a la no Conexión de Campos Seleccionados.- *Provee la integridad de campos elegidos entre los datos de una comunicación sin conexión.*

1.6.1.1.5) No Repudio

El no repudio proporciona protección en contra de la posibilidad que alguna de las partes involucradas en una comunicación niegue haber enviado o recibido un mensaje.

Las disputas resultantes [X.81397] sólo pueden resolverse con la disponibilidad de las pruebas. Éstas pueden ser resueltas directamente por las partes involucradas o por un árbitro.

El arbitraje sólo puede ser eficaz si las partes involucradas aceptan la autoridad del árbitro y solamente las evidencias aportadas son aceptadas si están garantizadas por una o más terceras partes confiables. (Facultativamente, el árbitro puede ser la tercera parte confiable).

Los mecanismos de no repudio utilizan varios tipos de terceras partes confiables y formas de evidencia como lo son la fecha, la hora y ubicación del originador/receptor.

No repudio con Pruebas de Origen

*Las pruebas del origen de los datos son entregadas al destinatario para protegerlo en contra de que el remitente tratase de impugnar falsamente algún dato o contenido enviado; incluso contra la falsa afirmación por parte del originador de que los datos no fueron los que se enviaron [*X.81397*]*.

No repudio con Pruebas de Entrega

Las pruebas de la recepción de los datos o su contenido son entregadas al remitente para protegerlo en contra de que el destinatario no niegue la recepción de dichos datos o su contenido o contra la falsa afirmación de que los datos recibidos no son como se enviaron, es decir, que hayan sido modificados por parte del receptor.

1.6.1.1.6) Disponibilidad

El análisis de la disponibilidad que se refiere a los datos y al servicio, es algo complejo en su estudio como servicio de seguridad; el ISO 7498-2 y la Recomendación ITU-T X.800 **no consideran a la disponibilidad como un servicio de seguridad.**

Por otro lado el triángulo CIA (CIA triad – Confidenciality Integrity Availability) afirma que la Tecnología de la Información (TI) es basada en tres objetivos de seguridad: confidencialidad, integridad y disponibilidad; pero no hay justificación para ella. Más sin embargo hay evidencias en contra, las cuales indican que dicha afirmación puede ser incorrecta. Dos argumentos son explicados:

Primero, ¿es realmente cierto que la seguridad en la TI sólo tiene 3 objetivos: Confidencialidad, Integridad y Disponibilidad?

En este trabajo hemos explicado que el estándar ISO 7498-2 ó la Recomendación ITU-T X.800 identifican por lo menos 5 servicios de seguridad y hay otros que argumentan que hay más [Donn91].

Segundo, ¿verdaderamente la disponibilidad es un objetivo de la seguridad?

Por décadas, los profesionales de la TI han usado el término "*disponibilidad*" en el sentido de "la probabilidad que el sistema estará funcionando correctamente en algún tiempo dado [Storey96]". Y cuando los profesionales de la seguridad de la TI se apropiaron del término le dieron uno nuevo, diferente y con un significado más reducido: "protección en contra de la denegación de servicio". Esto provocó una confusión y finalmente consiguieron que numerosos profesionales de seguridad de TI aparentemente ahora crean que su trabajo es lograr la disponibilidad en el amplio sentido de la palabra.

Ahora si intentásemos construir una justificación para la afirmación de que la disponibilidad es un objetivo de seguridad, podríamos analizar la siguiente tabla (Tabla 1) y determinar lo siguiente:

	LECTURA	ESCRITURA	RETENCIÓN DE LECTURA/ESCRITURA
Protección de los datos en contra de un no autorizado …	Confidencialidad	Integridad	"Disponibilidad" [= Protección en contra de la Denegación del Servicio]

Tabla 1.- Protección en contra de Condiciones Negativas

La revelación y la alteración de la información respectivamente corresponden a la confidencialidad y a la integridad, que a su vez se relacionan a los dos modos fundamentales de acceso a la información en sistemas automatizados, *lectura* y *escritura.* Si además tratásemos de agregar a la disponibilidad, primero debemos acotar el término *disponibilidad* como la "protección en contra de la denegación de servicio".

Aquí la noción es defender en contra de alguien que no este autorizado para denegar a los usuarios el acceso a la información para los cuales ellos están autorizados. Entonces, la retención de la lectura y escritura podemos tomarla como un metanivel.

Sin embargo, para construir una justificación más completa necesitaríamos más argumentos. Simplemente se concluye que hay una amplia razón para dudar acerca de la afirmación de que la disponibilidad deba actuar como un servicio de seguridad.

1.6.1.2) Mecanismos de Seguridad

Un mecanismo de seguridad es un procedimiento concreto utilizado para implementar un servicio de seguridad. En otras palabras, describe *cómo lograr* un servicio de seguridad.

1.6.1.2.1) Mecanismos de Cifrado

Es el proceso de codificar un mensaje para que su significado no sea evidente [Pfleeger96].

Los algoritmos de cifrado pueden ser reversibles o irreversibles.

Reversibles:

- Cifrado Simétrico (Llave Secreta).- En el cual el conocimiento del cifrado de llaves implica el conocimiento de la llave de descifrado y de cifrado.
- Cifrado Asimétrico (Llave Pública).- En el cual el conocimiento de la llave de cifrado no implica el conocimiento de la llave de descifrado, o viceversa. Las dos llaves del sistema son algunas veces mencionadas como "llave pública" y "llave privada".

Irreversibles:

Pueden o no pueden usar una llave. Cuando usan una llave, esta llave puede ser pública o privada.

La existencia de un mecanismo de cifrado implica un mecanismo de administración de claves, excepto en el caso de algunos algoritmos irreversibles.

1.6.1.2.2) Mecanismos de Firma Digital

La clave de este mecanismo es que la firma solamente puede ser producida usando la información privada del firmante.

Cuando la firma es verificada, podría ser corroborada subsecuentemente por una tercera parte confiable; por ejemplo un juez o un árbitro.

Este mecanismo define dos procedimientos:

- Firmando una unidad de datos, y
- Verificando una unidad de datos firmada

El primer proceso usa información privada (única y confidencial) al firmante.

El segundo proceso usa procedimientos e información los cuales son públicamente disponibles pero desde los cuales la información privada del firmante no puede ser deducida.

1.6.1.2.3) Mecanismos de Control de Acceso

El proceso para determinar cuál es la utilización permitida de los recursos de un entorno en un sistema, así como la prevención de los accesos no autorizados, se le denomina *control de acceso*. Éstos están relacionados con numerosos tipos de entidades que intentan acceder o utilizar los recursos, tales como:

- Entidades físicas
- Entidades lógicas
- Usuarios humanos

Los accesos pueden ser *a* un sistema (es decir, a una entidad que es la parte que se comunica de un sistema) o *dentro* del sistema. Algunas entidades del sistema involucradas en ser protegidas pueden ser:

- Una entidad de capa del modelo OSI
- Un archivo
- Un sistema

Si la entidad trata de usar un no autorizado recurso, o un autorizado recurso con un impropio tipo de acceso, llámese divulgación, modificación, destrucción o denegación de servicio [X.81296], las restricciones en el control de acceso deben rechazar el intento.

1.6.1.2.4) Mecanismos de Integridad de Datos

Se pueden entender dos tipos de servicios de integridad:

- La integridad de una simple unidad de dato o campo; y
- La integridad de una cadena de unidades de datos o campos.

Determinar la integridad de una simple unidad de dato envuelve dos procesos; uno en la entidad emisora y uno en la entidad receptora.

La entidad emisora agrega una función de sus propios datos en la unidad de datos enviada. Esta información extra puede ser un código de verificación de bloques o un verificador de valor criptográfico y puede además ir cifrado. La entidad receptora genera su correspondiente función complementaria y la compara con los datos recibidos para determinar si el dato ha sido modificado en tránsito.

1.6.1.2.5) Mecanismos de Intercambio de Autenticación

Algunas técnicas son:

- Uso de información de autenticación; como claves las cuales son suministradas por una entidad emisora y verificadas por una entidad receptora.
- Técnicas criptográficas.
- Uso de características y/o posesiones de la entidad y/o por su localización.

Si el mecanismo no es exitoso el resultado obtenido podría ser el rechazo o la terminación de la conexión.

Cuando técnicas criptográficas son utilizadas, ellas pueden ser combinadas con protocolos "*hand-shaking*" o *"de saludo inicial"*.

La elección de técnicas de intercambio de autenticación dependerá sobre las circunstancias en las cuales ellas sean necesitadas. En muchas circunstancias ellas deberán ser complementadas con:

- Estampados de hora y sincronización de relojes.
- Protocolos de Saludo Inicial de dos o tres caminos (autenticación unilateral o mutua).
- Servicios de no repudio realizados por mecanismos de notarización y/o firma digital.

1.6.1.2.6) Mecanismos de Protección contra Análisis de Tráfico

Pueden ser usados para proveer varios niveles de protección en contra del análisis de tráfico. Este mecanismo puede ser efectivo solamente si es protegido por un servicio de confidencialidad.

1.6.1.2.7) Mecanismos de Control de Enrutamiento

Las rutas pueden ser implementadas o dinámicamente o pueden ser pre asignadas; estas últimas son utilizadas para robustecer subredes, transmisiones o enlaces.
Se puede especificar al proveedor del servicio de red para que establezca una conexión vía una diferente ruta. Los datos con ciertas etiquetas de seguridad pueden ser prohibidos por una cierta política de seguridad para que sólo pasen por ciertas subredes, transmisiones o enlaces.

También el iniciador de una comunicación puede especificar advertencias de encaminamiento para que específicas subredes, enlaces o transmisiones sean evitados.

1.6.1.2.8) Mecanismos de Notarización

Propiedades acerca del dato comunicado entre dos o más entidades, tales como su integridad, origen, tiempo y destino, pueden ser aseguradas por el suministro de un mecanismo de notarización.

La certeza es provista por una tercera parte confiable: un notario; el cual es confiable por las entidades comunicándose, y el cual mantiene la información necesaria para proveer la certeza requerida de una manera justificable.

Cuando el mecanismo de notarización es invocado, el dato es comunicado entre las entidades comunicándose vía las protegidas instancias de comunicación y el notario.

1.6.1.3) Ilustración de la relación entre los Mecanismos, Servicios y Capas

A continuación se presentan dos tablas (Tabla 1 y 2) en las que se muestran los servicios de seguridad que se implementan en cada capa, conforme a la arquitectura definida en el modelo OSI, así como los mecanismos de seguridad empleados para implementar cada servicio.

Servicio de Seguridad	Mecanismos							
	Cifrado	Firma Digital	Control De Acceso	Integridad	Autenticación	Traffic Padding	Control de Ruteo	Notarización
Autenticación de indentidad	Si	Si			Si			
Autenticación de origen de datos	Si	Si						
Control de acceso			Si					
Confidencialidad con conexión y sin conexión	Si						Si	
Confidencialidad selectiva de campo	Si							
Confidencialidad de flujo de tráfico	Si					Si	Si	
Integridad con conexión con o sin recuperación	Si			Si				
Integridad con conexión selectiva de campo	Si			Si				
Integridad sin conexión	Si	Si		Si				
Integridad sin conexión y selección de campo	Si	Si		Si				
No repudio: origen y entrega		Si		Si				Si

Tabla 2.- Relación entre servicios y mecanismos de seguridad

Servicio de Seguridad	CAPA						
	Física 1	Enlace 2	Red 3	Transporte 4	Sesión 5	Presentación 6	Aplicación 7
Autenticación de indentidad			Si	Si			Si
Autenticación de origen			Si	Si			Si
Control de acceso			Si	Si			Si
Confidencialidad con conexión	Si	Si	Si	Si			Si
Confidencialidad sin conexión		Si	Si	Si			Si
Confidencialidad selectiva de campo							Si
Confidencialidad de flujo de tráfico	Si		Si				Si
Integridad con conexión y con recuperación				Si			Si
Integridad con conexión y sin recuperación			Si	Si			Si
Integridad con conexión selectiva de campo							Si
Integridad sin conexión			Si	Si			Si
Integridad sin conexión selectiva de campo							Si
No repudio con prueba de origen							Si
No repudio con prueba de entrega							Si

Tabla 3.- Relación entre servicios de seguridad y las capas del modelo OSI

Como se ha podido observar en las Tablas 2, cuatro de los cinco servicios de seguridad que estandariza el ISO 7498-2 se implementan

usando técnicas criptográficas, por lo que la seguridad informática está íntimamente relacionada con la criptografía.

1.6.1.4) Interacciones entre Mecanismos de Seguridad

A veces se necesitan diferentes servicios de seguridad en una comunicación; esta necesidad se puede cubrir utilizando o un solo mecanismo de seguridad que proporcione múltiples servicios de seguridad, o simultáneamente diferentes mecanismos.

Por ejemplo; pensemos en una comunicación donde Alicia deba enviar ciertos datos a Bob. Bob debe estar seguro que la información realmente la está enviando Alicia (autenticación), así como también le preocupa conocer que la información le sea llegada sin ningún tipo de alteración (integridad). Por otro parte, las políticas en la transferencia de datos, dictan que todos los datos que pasen sobre un Router, deberán ser verificados en su integridad.

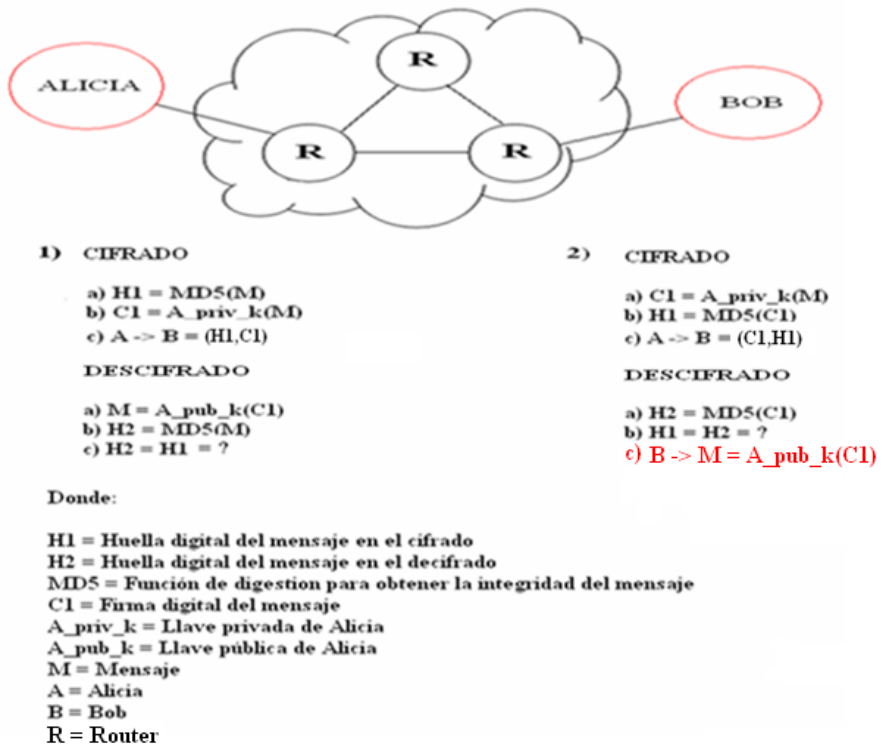


Figura 3.- Comunicación entre Alicia y Bob

Dos opciones son ejemplificadas en la Figura 3

1) CIFRADO
    a. Obtenemos H1 por medio de M.
    b. Obtenemos C1 por medio de M.
    c. Se envían ambas: H1 y C1.

   DESCIFRADO
    a. Desciframos C1 con A_pub_k para obtener M y garantizar la autenticidad de que Alicia nos envió dicha información.
    b. Obtenemos la huella digital desde M.
    c. Comparamos las huellas digitales para verificar la integridad.

2) CIFRADO
    a. Obtenemos C1 por medio de M.
    b. Obtenemos H1 por medio de C1.
    c. Se envían ambas: C1 y H1.

   DESCIFRADO
    a. Obtenemos H2 por medio de C1.
    b. Comparamos H1 con H2 para obtener la integridad de la información.
    c. Bob toma A_pub_k para obtener M y con ello autenticar a Alicia.

Podemos observar que ambos ejemplos satisfacen dicho problema; pero siendo cuidadosos al analizar el ejemplo uno, podemos comentar lo siguiente:

- Cualquier R por donde pase M es visto; ya que es necesario conocer el texto en claro M para subsecuentemente obtener la huella digital H1.
- Es necesario tener acceso a la llave pública de Alicia para obtener M.
- Cada R debe autenticar a A, aunque no sea un requisito del problema.

A lo que en el ejemplo dos, podemos partir del supuesto en que sólo Alicia y Bob puedan tener acceso a sus llaves públicas; al final solamente Bob autenticará a Alicia y por supuesto, ningún Router jamás tendrá conocimiento del texto en claro M.

Concluimos que: Las propiedades de seguridad de los mecanismos dependen del orden en el cual se combinarán las transformaciones criptográficas. Es de suma importancia analizar la interacción entre

los mecanismos de seguridad a usar, pues un mal análisis podría traer catastróficas vulnerabilidades al sistema, el uso de mayores recursos; tanto físicos como lógicos, sobrecarga de procesamiento en los equipos, sobrecarga innecesaria en el ancho de banda, etc.

1.6.1.5) Otros Mecanismos de Seguridad

Los siguientes mecanismos no son específicos para algún servicio en particular, es por eso que no son explícitamente descritos para una determinada capa en el Modelo de Referencia OSI. Éstos más bien deben de ser implementados según el nivel de seguridad que se requiera.

1.6.1.5.1) Funcionalidad de Confianza

Estos procedimientos en general son costosos y difíciles de implementar. Prácticamente se refiere a alguna funcionalidad la cual directamente provea, una situación de confianza.

La funcionalidad de confianza debe ser usada para extender la efectividad de otros mecanismos de seguridad. Los procedimientos tanto en software como en hardware varían dependiendo el nivel de amenazas percibidas y el valor de la información a ser protegida.

1.6.1.5.2) Etiquetas de Seguridad

Los recursos incluyendo los datos pueden tener etiquetas de seguridad asociadas con ellos. Por ejemplo para indicar un nivel de sensibilidad.

Una etiqueta de seguridad puede ser un dato adicional asociado con el dato transferido o puede ser algo relacionado implícitamente; por ejemplo, el uso de una clave específica para cifrar datos; o por el contexto de un dato, como su origen o su ruta de transferencia.

1.6.1.5.3) Detección de Eventos

Incluye la detección de consideraciones relacionadas con la seguridad [X.73692]. Puede incluir también la detección de eventos normales:

- Ingresos exitosos a los sistemas
- Específicas violaciones de seguridad
- Específicos eventos elegidos
- Exceso de ocurrencias sobre un evento

La detección de varios eventos relevantes a la seguridad pueden por ejemplo, causar una o más de las siguientes acciones:

- Informe local o remoto en tiempo real del evento
- Registro del evento
- Acción de recuperación

1.6.1.5.4) Pistas de Auditoría de Seguridad

Una auditoría de seguridad es una independiente revisión y examinación de registros y actividades del sistema que proveen un valioso mecanismo para la detección y la investigación de posibles brechas de seguridad con el fin de determinar que información u otros recursos han sido comprometidos.

Los objetivos de una auditoría de seguridad son los siguientes [X.81695]:

- Facilitar la identificación y el análisis de las acciones o ataques no autorizados;
- Ayudar a garantizar que las acciones puedan atribuirse a las entidades responsables;
- Contribuir al desarrollo de los procedimientos mejorados del control de daños;
- Confirmar el cumplimiento de las políticas de seguridad;
- Notificar cualquier información que pueda indicar insuficiencias en los controles del sistema; y
- Determinar los posibles cambios necesarios de controles, política y/o procedimientos.

La conocida existencia de pistas de auditoría de seguridad puede ser un factor disuasivo para aquellos individuos que pudieran intentar dañar el sistema.

Los mecanismos de auditoría de seguridad no participan directamente en la prevención de las violaciones de seguridad; únicamente están relacionados con la detección, el registro y el análisis de eventos.

En muchos países existen leyes destinadas a proteger la privacidad de los ciudadanos. Un registro de rastreo personal puede verse afectado por las leyes nacionales, relacionadas con la privacidad y el acceso a la información. Tales registros deberán ser protegidos contra la información no autorizada.

En aquellos casos en que los registros de auditoría de seguridad se utilicen como evidencia legalmente admisible, pueden existir requisitos específicos con respecto a la utilización, almacenamiento y protección de los registros de auditoría de seguridad.

1.6.1.5.5) Recuperación de la Seguridad

Apoyado con otros mecanismos como la manipulación de eventos y la administración de funciones, acciones de recuperación son llevadas a cabo.

Estas acciones de recuperación pueden ser de tres tipos:

- Inmediatas.- Acciones inmediatas pueden crear una inmediata suspensión de las operaciones, como una desconexión.
- Eventuales.- Pueden producir una temporal invalidación de una entidad.
- Largo término.- Pueden ser la introducción de una entidad dentro de una "lista negra" o el cambio de una clave.

1.6.1.5.6) Alarmas de Seguridad

El usuario de la gestión de seguridad necesita ser avisado siempre que se detecte un evento indicador de un ataque. Un ataque contra la seguridad puede ser detectado por un servicio, un mecanismo o por otro proceso.

El estándar ISO 7498-2 ó la Recomendación ITU-T X.800 **no definen** a las alarmas de seguridad como mecanismos de seguridad, sino como acciones identificadas por las políticas de seguridad como posibles brechas de seguridad [X.73692].

Una notificación de alarma de seguridad puede ser generada por uno de los usuarios finales comunicantes o por cualquier sistema o proceso intermedio situado entre los usuarios finales. Algunos de

estos eventos pueden requerir una acción inmediata, mientras que otros pudieran requerir una investigación ulterior para determinar alguna acción requerida, si así lo necesitase.

En la tabla 4 se indican las causas de alarma de seguridad correspondientes a los tipos de informe de seguridad específicos.

Tipo de evento	Causas de alarma de seguridad
Violación de la integridad	Información duplicada Información faltante Detección de modificación de información Información fuera de secuencia Información no esperada
Violación operacional	Denegación de servicio Fuera de servicio Error de procedimiento Razón no especificada
Violación física	Manipulación de cable Detección de intrusión Razón no especificada
Violación de servicio o de mecanismo de seguridad	Fallo de autenticación Brecha en la confidencialidad Fallo de no repudio Intento de acceso no autorizado Razón no especificada
Violación del dominio temporal	Información retardada Clave caducada Actividad a deshora

Tabla 4.- Causas de Alarmas de Seguridad

Al término de este capítulo se puede comprender ampliamente que nuestro sistema para el reconocimiento del caminar humano debe ser analizado y modelado en escenarios particulares donde se pretenda implementar este tipo de tecnología; pues, como ahora ya sabemos, no hay un modelo de seguridad específico a seguir en todos los escenarios. Es por eso que se requiere hacer un análisis específico de seguridad en cada escenario para saber en contra de qué se va a proteger, qué se va proteger y como se van a proteger nuestros activos.

Así mismo podemos comprender que para que una persona la podamos identificar al caminar, debemos completamente verificar la identidad de esa persona para que se garantice que ella es quien ella

dice ser; y por tanto, se cumpla con el objetivo que se describirá en el siguiente capítulo: el servicio de autenticación

En el mundo digital si queremos amarrar un evento a un individuo, es importante que nosotros apropiadamente amarremos al individuo a su identidad digital.

"Anónimo"

II AUTENTICACIÓN

2.1) INTRODUCCIÓN

La autenticación se refiere a ***la verificación de tu identidad*** y la autenticación responde a la pregunta de *"¿Quién tú eres?".*

Antes de las telecomunicaciones y las redes de computadoras, el modo tradicional de autenticación era por medio de un guardia. Cuando un guardia visualmente reconocía a la persona que solicitaba la autenticación y sabía que él era el autorizado, el guardia otorgaba la autenticación. Sin embargo, hoy en día para transacciones remotas se utilizan derivados indicadores de la autenticidad; ellos no son *"¿Quién tú eres?",* pero un manualmente acordado dispositivo o protocolo actúa como evidencia de *que tu eres quien tú dices ser* [O´Gorman04].

La autenticación humana es tratar de limitar el acceso a las redes computacionales o a las ubicaciones físicas solamente a las entidades que tengan autorización verificando la identidad y determinando la legitimidad de un individuo. Esto es hecho, equipando a los usuarios con algún método de autenticación como lo es: un NIP (Número de Identificación Personal), un testigo[1], un biométrico, un aparato SPG o cualquier combinación que se pudiera realizar con cualquiera de los anteriores. Sin embargo debido a la imperfección humana o a la poca cultura que se tenga, estos no siempre son usados con las debidas precauciones, debido a los hoyos de seguridad que se van dejando, o ellos son demasiado seguros, pero inconvenientes para las circunstancias.

Los métodos de autenticación son las herramientas que nos ayudan a conseguir el acceso que puede ser otorgado. Sin embargo, estas herramientas no son equivalentes, y desafortunadamente todavía ninguno ha probado tener certeza en ofrecer una "perfecta seguridad" y una conveniencia universal [O´Gorman04].

El primer método de autenticación conocido era la autenticación hombre-a-hombre, pero con el nacimiento de las computadoras y las telecomunicaciones surge la necesidad de un funcionamiento entre comunicaciones más confiable. Ahora tres métodos generales de

[1] Pequeño dispositivo físico que un usuario autorizado de servicios de cómputo se le es dado para ayudar a una autenticación, en el inglés es conocido como "token".

autenticación son conocidos: hombre-a-hombre, hombre-a-maquina y máquina-a-máquina[2].

Por lo tanto, en nuestra investigación solamente vamos a retomar dos métodos de autenticación como lo vemos en la figura 4: Hombre-Máquina y Máquina-Máquina.

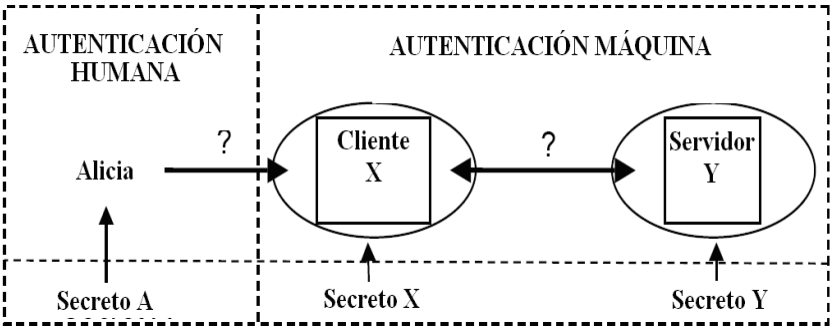


Figura 4.- Autenticación Hombre-Máquina y Máquina-Máquina

2.2) FASES DE LA AUTENTICACIÓN

2.2.1) Registro

Cualquier sistema que pretenda hacer uso de mecanismos de identificación y/o autenticación requiere de un procedimiento de registro de las componentes del mismo. Hay que levantar un inventario de componentes y/o de usuarios. El sistema se considera acotado a los elementos que consten en este inventario, y aquellos elementos que no aparezcan en este inventario, por definición, no forman parte del sistema. Claro, este inventario se modifica a lo largo del tiempo, estando sujeto a procesos de altas, bajas y cambios.

.

Un ejemplo de un registro es cuando tratamos de ingresar a una computadora con un acceso delimitado. Si la computadora tiene un control de acceso, hay que acudir al administrador del sistema para solicitar una cuenta de usuario; procedimiento que no es más que el registro a un sistema que está formado por todos los miembros que puedan tener acceso a la computadora. El solicitante entonces pide usar el sistema y el administrador da de alta al usuario y debe entregar su correspondiente clave de acceso. Al solicitar ingreso en el sistema, se deben de mostrar las credenciales como prueba de la realización del registro.

[2] Existen métodos para autenticar animales u objetos, pero este documento hace referencia al humano.

2.2.2) Identificación

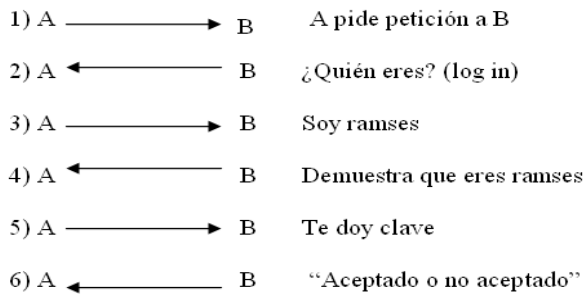
En el registro en cualquier sistema se anota un identificador del usuario. Este puede ser su nombre, un apodo, un número (como en las cuentas numeradas de ciertos bancos, o el número de pasaporte) o información que distinga a un usuario de los demás. Mediante este identificador se localiza al correspondiente usuario.

2.2.3) Autentificación

Al registrarse el usuario debe depositar o recibir algo que lo autentique, que es un dato que se relacione con el usuario. *La posesión de este dato se considera como evidencia incontrovertible de que el que lo exhibe es quien aparece en el registro.* La imposibilidad de exhibir el dato que autentica, inmediatamente lleva a la denegación del uso del servicio que se solicita.

En el caso del ingreso a la computadora con acceso delimitado, la identidad se demuestra mediante el nombre del usuario. Este nombre es una identificación mediante la cual el sistema acredita quien va a usar el sistema. Como apoyo a este elemento de identidad se incluye un elemento que es una clave de acceso. Esta clave es verificada por la computadora y hace constar la identidad del usuario. La clave por tanto, debería indicar que el usuario ha llevado a cabo el trámite de registro ante el administrador del sistema.

Para que estos términos queden más claros, nos basaremos en el protocolo[3] de Unix; el cual lo enfocaremos sobre estos tres puntos:



[3] Un protocolo es una *secuencia preacordada de acciones para lograr alguna tarea.*

- **Punto 1.** En este ejemplo podemos ver que en el paso tres el usuario ramses (A) se tiene que identificar ante el sistema (B).
- **Punto 2.** En el paso cinco el usuario ramses (A) se tiene que autenticar con el sistema (B).
- **Punto 3.** Y para todo este protocolo tuvo que haber un registro preestablecido para formar parte del sistema.

2.3) MÉTODOS DE AUTENTICACIÓN

Los cuatro métodos de autenticación o categorías de características usadas hoy, son:

- *Alguna cosa que se conoce:* NIP, contraseña, o información personal tal como el nombre de soltera de mamá, etc..
- *Alguna cosa que se tiene:* Una tarjeta de crédito, una llave, etc..
- *Alguna cosa que se es:* Una característica personal tal como una huella digital, una firma, reconocimiento de voz, etc..
- *Algo basado en la ubicación:* Caracterizada por satélites.

2.3.1) Alguna cosa que se conoce

Este tipo de herramienta de autenticación está basado en un secreto compartido por el usuario y el sistema de información. Típicamente se trata de una contraseña, que es una palabra o más generalmente una sucesión de caracteres alfanuméricos.

Cuando un usuario se identifica al solicitar acceso a un sistema de información, debe además exhibir su contraseña, que está registrada en el archivo de usuarios del sistema. Esta contraseña se asigna en el momento de su registro, pero puede ser cambiada tantas veces como el usuario desee.

2.3.2) Cosas que se conocen que pueden ser descubiertas, predichas o pirateadas

Puesto que se trata de un secreto compartido, hay que proteger este secreto en ambos extremos de la trayectoria. O sea, en el archivo de usuarios y en la memoria de la persona que lo usa. También hay que proteger el secreto en el tránsito del usuario al sistema. La mayor parte de las intrusiones se deben a una protección deficiente en alguno de estos puntos. Si alguien ajeno al sistema llega a conocer el

secreto compartido puede suplantar al usuario y dejar de estar fuera del sistema.

Los requerimientos en la fortaleza de las contraseñas pueden ser impuestos al usuario, pero si la contraseña es muy difícil, el usuario puede escribir la contraseña más sencilla en un esfuerzo por no olvidarla. Sin imponer alguna fortaleza o requerimiento al secreto, los usuarios pueden crear una contraseña que es fácil de recordar o predecir. Esto hace el trabajo de los piratas informáticos y la tecnología de las intrusiones a las contraseñas más fácil. Incluso, muchas personas vuelven a usar la misma contraseña para diferentes accesos; por lo tanto si una contraseña es comprometida, todos los demás accesos pueden ser comprometidos.

Para entender las precauciones que hay que tener para proteger el secreto compartido hay que reflexionar sobre las posibles acciones de un suplantador en potencia.

Si el suplantador logra enterarse del secreto porque el usuario lo escribió y no ocultó ese escrito, no hay defensa posible. Lo único que se puede hacer es convencer a los usuarios de que no escriban su contraseña en un documento público[4], y seleccionar la contraseña en forma nemónica, para que el usuario la recuerde sin necesidad de escribirla.

Si el suplantador logra obtener el archivo de usuarios que residen en el sistema y en éste aparecen sus contraseñas, los intentos de autenticación serían inmediatos y no habría ningún tipo de defensa. Lo que se debe hacer, es, NO almacenar las contraseñas en claro en el archivo de usuarios, sino almacenarlas en forma cifrada.

No es buena práctica transmitir la contraseña en una comunicación, pues el suplantador puede percibirla, lo que hay que hacer es NO transmitirla. En lugar de hacerlo, el sistema puede cifrar algún mensaje con la contraseña y enviar el mensaje cifrado. A su vez el usuario hace algo similar devolviendo su mensaje original añadiendo otro mensaje y cifrando el conjunto con la contraseña. El sistema al

[4] El usuario puede crear un archivo en la computadora con una lista de identificadores y sus propias contraseñas, donde sólo él "pueda" tener acceso a ese archivo. Los usuarios pueden además mantener una copia de respaldo por ejemplo en el correo electrónico, pero cifradas con una clave única o resguardadas bajo un testigo del cual se hablará más adelante [15].

recibir su propio mensaje descifrado logra la autenticación del usuario. Hay diversas variantes de este procedimiento llamados "protocolos de autenticación fuerte basados en contraseñas débiles".

Si el suplantador obtiene un archivo con contraseñas cifradas y conoce el algoritmo de cifrado, puede emplear todas las combinaciones posibles de los caracteres lícitos, cifrarlas, y producir así una lista de contraseñas posibles que puede probar una por una.

El suplantador además, puede intentar adivinar la contraseña de un usuario, mediante una lista de contraseñas probables. Puede usar listas exhaustivas o aprovechar la tendencia natural a usar contraseñas nemónicas y elaborar una lista de contraseñas probables (nombre del usuario, nombre de la esposa, del perro, fecha de nacimiento, etc.) basadas en su conocimiento del usuario. También se puede emplear una lista de palabras frecuentes del idioma empleado por el usuario. Una por una las presenta al sistema en repetidos intentos para obtener acceso.

Algunas soluciones pueden ser limitar el número de intentos que se permiten, alertando al administrador cuando se exceda este límite. También se puede limitar el tiempo durante el cual se permite solicitar acceso al sistema.

Las contraseñas más largas (ocho o más caracteres es lo recomendable) son más difíciles de adivinar o de producir cifrando combinaciones.

Todos los ataques que hemos mencionado toman tiempo, y su éxito persiste en la medida que la contraseña no cambie. Es pues una precaución recomendable cambiar la contraseña periódicamente, pudiéndose llegar al extremo de cambiar la contraseña cada vez que se ingresa al sistema.

Como los usuarios pueden cambiar la contraseña cuando les plazca, se deben revisar éstas automáticamente. Hay que vigilar que existan (pues se han dado casos de usuarios que quitan su contraseña), que tengan la longitud adecuada y que estén conformadas según las políticas de la organización.
El secreto compartido no se limita necesariamente a una palabra o a un conjunto de caracteres. En el momento de registro el usuario

puede proporcionar una serie de datos en forma de preguntas y respuestas que probablemente solo él reconoce. Es decir quizás otras personas conozcan algunos de los datos, pero no todos ellos. Por ejemplo nombres de ancestros, fechas significativas, gustos y fobias, etc. El sistema almacena esta serie de datos, y le solicita al usuario, mediante una selección aleatoria de preguntas de esta lista de datos, que proporcione respuestas. Todas las respuestas deben ser apropiadas para que se considere que el usuario se ha autenticado. La serie de preguntas y respuestas deben almacenarse de forma segura en el sistema para evitar que un suplantador las obtenga.

La información personal es predecible o fácil de encontrar por eso llegamos a la conclusión de que ***"no es totalmente confiable".***

El ladrón puede ser alguien que conoces quien tiene fácil acceso a tu historial o información de cuenta. Es estimado que más de la mitad de toda la documentación de identidad robada es cometida por criminales que han establecido relaciones con sus víctimas, tales como familiares, compañeros de cuarto, vecinos, compañeros de trabajo, etc..

2.3.3) Alguna cosa que se tiene

Una tarjeta u objeto inteligente, es decir que tenga un procesador y memoria, se puede emplear como una herramienta de autenticación. Por ejemplo, para evitar transmitir en claro la contraseña del usuario, un dispositivo inteligente puede cifrarla para su posterior transmisión, o inclusive la puede transmitir directamente, participando en algún protocolo que evite los ataques de retransmisión de información interceptada. Otra posibilidad es que el dispositivo genere contraseñas con mucha frecuencia, digamos cada 30 segundos, en forma sincrónica con el sistema al que permite acceso. De esta manera el dispositivo y el sistema comparten un secreto nuevo cada 30 segundos. Pueden también emplearse en protocolos de tipo "santo y seña" no verbales sino digitales en los cuales el dispositivo y el sistema intercambian "preguntas" y "respuestas" predeterminadas, o determinadas algorítmicamente.

Los dispositivos que se emplean para este propósito son tarjetas inteligentes (similares a las bancarias), anillos java o tarjetas que se insertan en una computadora. Si se emplean objetos portátiles se pueden perder o dañar, impidiendo al usuario el acceso. Si no se fabrican con mucho cuidado son susceptibles a la clonación, es decir,

a la producción de copias idénticas que son igualmente efectivas para facilitar el acceso al sistema.

Los dispositivos físicos que permiten la autenticación de los usuarios de un sistema contienen información relativa a su dueño o a la actividad que se pretende realizar. Esta información, además de servir como herramienta de autenticación, puede ser usada para otros fines. Por ejemplo puede ser el historial clínico de un usuario, o su información bancaria; inclusive puede ser efectivo electrónico para efectuar pagos.

Si estos dispositivos se usan remotamente, es decir fuera del lugar donde esté ubicado el sistema de información, corre el riesgo de que la autenticación del usuario no ocurra, sino simplemente la autenticación del dispositivo que puede estar en otras manos. La única forma de evitar esto es combinando las herramientas de autenticación basados en posesión con otras formas de autenticación[5].

2.3.4) Cosas que se tienen que pueden ser perdidas o robadas

Tarjetas de crédito, llaves, y algunas cosas que pueden estar dentro de este método de autenticación pueden ser perdidas o robadas. Por eso se llega a la conclusión de que **"no son totalmente confiables".**

2.3.5) Alguna cosa que se es

Aquí, la identidad se demuestra comparando patrones relacionados a alguna característica inherente a la naturaleza de la entidad que se identifica.

Se divide este método de autenticación en [Olsson03] dos vertientes: ***Los procesos que recaen sobre verificación manual y los procesos que recaen sobre verificación automatizada.***

Antes de las computadoras, esto podría haber sido una firma de una persona, un retrato, una huella, o una descripción de la apariencia física de una persona. Pero en los días de hoy, las características definidas de un individuo son calculadas, almacenadas digitalmente y comparadas contra patrones ya almacenados. Precisamente,

[5] Véase el apartado 2.5.

consiste en comparar alguna característica inherente a su naturaleza contra los patrones ya almacenados en el sistema. Técnicas relacionadas con los humanos ya bien conocidas y aún en investigación, usan la voz de una persona, la impresión de una huella, una firma escrita, la figura de la mano, la manera de caminar de las personas o características del ojo, entre otras, para su autenticación. Tales técnicas son conocidas como *sistemas biométricos.*

2.3.6) Algunas cosas que muchas veces recaen sobre verificación manual y otras vulnerabilidades sobre biometría

Un "sacador de borrachos" en un bar, mira la fecha de cumpleaños en la licencia de manejo y usa la fotografía para verificar que la licencia que se está usando sea de la persona quien la porta. Muchos de los métodos de verificación de uso cotidiano recaen sobre procesos manuales. Ellos son fácilmente erróneos u olvidados por la prisa de un buen servicio al cliente y pueden ser fácilmente falsificados.

Por otro lado, si hay una transmisión remota usando tecnología biométrica hay peligro de intercepción, ya que hay que tener en cuenta, que lo que siempre se transmite por una red, sea la tecnología que sea, son variaciones de voltaje, energía luminosa, señales electromagnéticas satelitales o de microondas y no hay nada que nos impida interceptar eso.

Además, como los aspectos biométricos son imposibles para ser modificados, el propietario no tiene camino para revertir los daños si el atacante roba el lector biométrico con los registros de los usuarios; o más grave aún, si alguien puede decir que ellos son yo y almacenar una muestra biométrica en mi nombre, entonces solo hemos dado al criminal un camino seguro para el robo de identidad, ya que un usuario no puede solicitar uno nuevo, como lo haría con una nueva clave o un nuevo número de tarjeta de crédito [Myers02].

Otra realidad que es un reto, es construir un preciso sistema lo suficientemente certero para denegar a los usuarios ilícitos sin esporádicamente denegar a los usuarios legítimos. Además de que los cambios fisiológicos o conductuales pueden hacer invalido al lector biométrico.

2.3.7) Algo que determina la posición en la Tierra

El Sistema Global de Posicionamiento (SGP) es un sistema de navegación de radio basado en satélites con la capacidad de rastrear la ubicación exacta sobre la tierra. Un SGP está compuesto de 3 elementos: Espacio de Segmento, Control de Segmento y un Segmento de Usuarios [Towson05].

Espacio de Segmento:

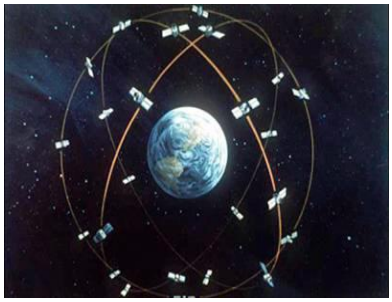


Figura 5.- Espacio de Segmento

Figura 5.- Es una constelación de 24 satélites que orbitan la Tierra dos veces al día, viajando a una velocidad arriba de las 700 millas por hora. Los satélites transmiten una señal precisa, la cual es detectada por los receptores SGP sobre la Tierra, dando la ubicación exacta del objeto.

Control de Segmento:

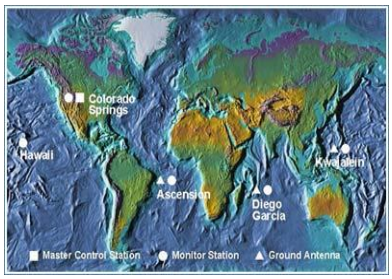


Figura 6.- Control de Segmento

Figura 6.- Es el sistema de rastreo. Hay 3 antenas y estaciones de monitoreo alrededor del mundo.

Segmento de Usuarios:

Figura 7.- Segmento de Usuarios

Figura 7.- La cual incluye todos los receptores SGP (dispositivos geoposicionadores) y la comunidad de los usuarios.

Los dispositivos geoposicionadores reciben estas señales y las usan para calcular la latitud, longitud y altura sobre el nivel del mar en que se encuentran.

La empresa Series Research ha desarrollado un dispositivo, llamado Cyberlocator, que lee las señales de los satélites de geoposicionamiento visibles en un punto y las transforma en lo que se llama una "firma de ubicación" (location signature).

La firma cuya longitud es de 20 kilobytes, incluye la hora (con precisión en milisegundos) en que se hicieron las observaciones. Esta firma depende de la posición y velocidad de los satélites observables.

[Olsson03] Esta firma se entrega a la computadora que se desea autenticar, y esta la transmite a través de Internet al servidor de autenticación. Este a su vez calcula su propia firma, usando los satélites que comparte con la que originó el proceso. El que ambas computadoras compartan varios satélites de la red, indica que no pueden estar a más de 3000 kilómetros de distancia. La comparación de firmas constituye una instancia de geoposicionamiento diferencial, que permite una localización con una precisión de menos de un metro. Si se desea una autenticación continua se puede calcular una firma cada 5 milisegundos, y la actualización de la autenticación sólo requiere 20 bytes por segundo.

Consecuentemente, hay una necesidad para dirigir alternativas. Una alternativa es implementar una autenticación basada en un esquema de adivinanza (puzzle-based) sobre la información de la ubicación. En el propuesto esquema [Rani05], el servidor realiza preguntas dinámicamente basadas en la ubicación y el cliente las responde basado sobre la propuesta ruta de viaje. Este esquema fortalece los actuales mecanismos de autenticación.

Una característica importante de este sistema es que identifica el lugar y el momento en que el dispositivo estuvo en ese lugar. Esto permite rastrear con mucha efectividad las posibles violaciones derivadas de una conexión a través de Internet. Es decir, que si se restringe el acceso a un sistema de información, se sabe donde estaban los usuarios conectados y cuando estaban ahí.

Además si la firma de ubicación se incluye en un documento se puede asegurar dónde y cuándo se creó el documento. También se puede evitar que un usuario legítimo se lleve información a un destino inapropiado. Otro uso de interés es saber desde donde se emitieron comandos que hagan cambios a sistemas de archivos, o que detengan la computadora, entre otros ejemplos.

El funcionamiento de este sistema NO requiere que el solicitante comparta un secreto con el otorgante de acceso. Pero si requiere del uso de un dispositivo en cada extremo. Por su naturaleza este sistema de autenticación se puede usar en forma bidireccional para establecer trayectorias confiables.

Por tanto, la razón fundamental de este método, es la posición geométrica entre los satélites en sus amplios ángulos relativos.

2.3.8) Algo que pueda atacar a la autenticación por determinada posición en la Tierra

No se puede falsificar debido a las perturbaciones orbítales que no son predecibles. Aparte que, confiar en la firma de ubicación impuesta por un satélite es muy confiable, pero tiene problemas como [Rani05]:

- La parte crítica de este esquema de autenticación son los SPG.
- No trabajará en los sótanos o desde el interior de grandes edificios donde la fuerza de la señal SPG no es buena.
- No hay SPG íntegros, es decir, la incapacidad de informar a los usuarios cuando el sistema no sea confiable.
- Errores orbitales ocurren cuando los satélites proveen información incierta.
- Si los SPG están en un lugar donde hay edificios altos, entonces las señales podrían retrasarse.
- El clima con cielo nublado y tormentoso adversamente afecta el potencial de esta técnica.

Este método es el más nuevo de los cuatro, es muy seguro pero el coste de implementación es muy alto.

2.4) COMPARACIÓN DE MÉTODOS DE AUTENTICACIÓN

A continuación haremos una comparación de los métodos de autenticación, basándome en [Bolle03], [Rani05], [GWilliams02], [O´Gorman04] y [Towson05].

Método		Ejemplo	Ventajas	Desventajas
Que tu sabes		Cuentas NIP Apellido del nombre de soltera de mamá Conocimiento personal	Rápido Barato No puede ser perdido físicamente	Las claves pueden fácilmente ser adivinadas El NIP es una colección débil (Escribiendo el NIP sobre una tarjeta) Puede ser olvidado, comprometido o compartido
Que tú tienes		Tarjetas Llaves de chapas	Muy difícil para abusar Evidencia de que está perdido Es más seguro que un NIP, por su universo de claves[6]	Puede ser compartido Puede ser duplicado Puede ser perdido Puede ser robado Coste alto Riesgo de fallas de hardware Debe recordar portarse
Alguna cosa que se es	Basado sobre verificación manual	Licencia de Manejo Credencial de Elector Tarjeta de Crédito	Barato Evidencia de que está perdido	Puede ser olvidado Puede ser compartido Puede ser duplicado Puede ser perdido o robado Debe recordar portarse
	Basado sobre un proceso automático	Manera de caminar Cara Iris Impresión de voz Retina	No es posible compartir Poco probable repudiar No puede ser perdido u olvidado Portátil	Caro Riesgos de privacidad Problemas con rechazos falsos o aceptaciones equivocadas Características pueden ser heridas
			Características no pueden ser cambiadas	
Algo que determina la posición en La Tierra		Firma de ubicación	No es posible falsificar o es casi imposible reemplazarlo Fiarse en las firmas de ubicación de los satélites es muy confiable	El mal tiempo La parte crítica recae absolutamente en los SPG Ángulos de los satélites Errores orbitales Visibilidad entre satélites

Tabla 5.- Características de los métodos de autenticación

La biometría por un proceso automatizado únicamente es susceptible a la falsificación [Dunker04], lo cual puede ser extremadamente difícil, dependiendo del tipo de biometría que se use. Algunos métodos también pueden ser susceptibles al robo, hablando de mutilaciones. Aunque ya existen sistemas biométricos que ya implementan autenticación con detección de muestras vivas[7].

[6] El "espacio de claves" o "keyspace" en inglés, es la extensión indefinida del conjunto de claves que existen en un determinado universo de claves.

[7] Si se desea un estudio más a fondo sobre algoritmos y sistemas que implementen autenticación con muestras vivas se puede consultar "Business Europe: Biometrics market begins to open up." EbusinessForum. 03 May 2002. URL: http://www.ebusinessforum.com/index.asp?layout=printer_friendly&doc_id=5647(10 Oct.2002).

En un protocolo de autenticación tres de los cuatro métodos de autenticación deben coincidir exactamente si son implementados por máquina. Sin embargo por necesidad, la biometría tiene que adoptar teoría probabilística y el uso de técnicas estadísticas para analizar la probabilidad de las coincidencias al momento de la autenticación, ya que éstas, pueden coincidir de una a más muestras.

Hay tres niveles básicos o escenarios de seguridad: conocimiento, posesión y biometría.

[GWilliams02] El nivel más bajo involucra alguna cosa que el usuario conoce, tal como una contraseña o un NIP. El siguiente nivel es alguna cosa que el usuario tiene, como una tarjeta ID. Combinando ambos hacen un más robusto sistema de seguridad y es la técnica usada por ejemplo en cajeros automáticos (ATMs). Sin embargo estos niveles fallan decisivamente para identificar o autenticar a un individuo. En contraste los sistemas biométricos basan la autenticación sobre características físicas [Olsson03] o conductuales; es decir, enlazan el proceso de verificación a un individuo, no a una tarjeta, o un número de cuenta, o a un NIP, o una contraseña, etc. (La combinación de un biométrico con un NIP o una clave es todavía más fuerte).

[Rani05] Consecuentemente, con el crecimiento de la tecnología inalámbrica en sectores como el militar y la aviación, hay una más fuerte necesidad para determinar la autenticidad de un usuario genuino donde una o más partes se están moviendo o necesitan moverse para ser implementadas. Tal solución es la autenticación basada en la ubicación, que considera la información de la ubicación de un usuario. La información de la ubicación es basada en el tiempo, por lo tanto es difícil de robar[8].

2.5) REFORZAMIENTO EN LA AUTENTICACIÓN

Cuando se combinan dos tecnologías se tienen factores adicionales de seguridad trabajando en conjunto para la necesidad de un ***alto nivel de seguridad.*** Ahora se tendría un segundo nivel de verificación para ayudar a proveer la autenticación.

[8]Para un estudio más completo sobre este método, por ejemplo para saber en ¿qué momento se puede usar? ó en ¿qué ocasión?, se puede consultar [Rani05], [O´Gorman04] y [Graham03].

Se le denomina un sistema de autenticación *multi*-factor; donde *multi* puede ser 2, 3 o 4, en un sistema que use exclusivamente *diferentes métodos de autenticación*. Aunque también encontramos el término *híbrido*, solo que aquí también se pueden agregar *herramientas de autenticación del mismo tipo*, como: huella digital con iris, o licencia de manejo con una firma de usuario y un NIP, etc..

Combinando múltiples métodos de autenticación dentro de un protocolo de autenticación, se refuerza la certeza y disminuyen las oportunidades de repudio y fraude [Bolle03].

Adecuando la autenticación por medio del hardware y el software ***se lograría además un ambiente más seguro.***

2.6) PUERTA TRASERA COMO PUERTA DE EMERGENCIA

Por las amplias vulnerabilidades que hemos descrito, y porque sabemos que el usuario no es perfecto. Surge la necesidad de poner una puerta trasera en las aplicaciones donde usemos cualquiera de los métodos de autenticación mencionados, como una segunda necesidad de control de acceso.

Para que esto quede más claro vamos a basarnos en un ejemplo que se encuentra en [DWilliams02]:

Por ejemplo en sistemas donde se usen tarjetas inteligentes muchas veces se usa la huella digital, no para autenticar, sino para desbloquear la tarjeta inteligente en el caso donde el usuario no pueda recordar su NIP. Solamente la huella digital del propietario de la tarjeta puede desbloquear la tarjeta.

Esto involucra que exista una nueva vulnerabilidad, a la cual le debamos tener sus propias precauciones de seguridad.

Podemos entender ahora que los 4 métodos de autenticación existentes tienen ventajas y desventajas y que ninguno es totalmente confiable pues se ha mencionado que cada uno tiene ciertos inconvenientes, pero que incluso se puede trabajar en conjunto entre diferentes tipos de autenticación para adecuar las exigencias del servicio de autenticación deseado.

Sin embargo, podemos notar algo; a excepción de la biometría, los demás métodos de autenticación se basan en identificar un ente no propio del individuo como lo es una tarjeta, una contraseña o un SPG y no a un individuo como tal.

Entonces, en este momento sabemos cómo se involucra un proceso de autenticación en un sistema, ahora entonces necesitamos saber cómo se comporta lo que nos interesa saber, la biometría como un proceso de autenticación.

La tecnología biométrica es definitivamente una espada de doble filo.

"David L. Sobel"

III BIOMETRÍA

3.1) INTRODUCCIÓN

La palabra biometría derivada de las palabras griegas bios (vida) y metron (medida) es tan antigua como el antiguo Egipto [Myers02]. Los individuos usaban rasgos característicos como cicatrices, peso, color de cabello u ojos, etc. para la realización de transacciones.

Las características físicas o del comportamiento son exclusivas para que un individuo sea autenticado. *Este modelo es el método más conveniente para la autenticación de individuos;* ya que los demás métodos de autenticación se basan en identificar un ente no propio del individuo como una tarjeta, una contraseña o un SPG y no a un individuo como tal.

La biometría envuelve el uso de diferentes partes del cuerpo, como una clave o forma de autenticación y se basa en la premisa de que cada persona es única y posee rasgos distintivos, ya sean físicos o conductuales que pueden ser utilizados para identificación o autenticación [GWilliams02]; y para eso se deben satisfacer ciertas características [Jain04]:

- **Universalidad.**– Cada una de las personas debería tener las características.
- **Distinción de Rasgos.-** Entre dos o más personas deben ser lo suficientemente diferentes para poder distinguirse.
- **Permanencia.-** Las características serían lo suficientemente invariantes sobre un periodo de tiempo.
- **Recolectadas.-** Las características pueden ser medidas cuantitativamente.

En seguridad informática, la biometría se refiere a las técnicas de autenticación que recaen sobre las medidas de las características físicas o conductuales, que pueden ser automáticamente verificadas. De aquí en adelante nos referiremos a la biometría, como un proceso automático y ya no, como un proceso que recae sobre verificación manual [Webopedia07].

3.2) FASES DE UN SISTEMA BIOMÉTRICO

Lógicamente un sistema biométrico puede ser dividido dentro de dos fases [Pankanti00]: el módulo de registro y el módulo de identificación o autenticación.

3.2.1) Módulo de Registro

El módulo de registro es el responsable de capacitar al sistema para identificar a una persona dada. Durante la fase de registro, un sensor biométrico escanea la fisonomía y/o el comportamiento específico de una persona para crear una representación digital. Una(s) característica(s) extraída(s) llamada(s) muestra(s) denominada(s) en inglés "sample(s)" procesa(n) esta representación para generar una más compacta y expresiva representación denominada "modelo[1]".

El modelo es otra característica importante en el análisis de una tecnología biométrica ya que el tamaño del modelo varía dependiendo del biométrico aplicado. En bases de datos donde hay demasiados usuarios, el tiempo de respuesta del sistema podría ser lento. Si el modelo es muy grande podría repercutir en el tiempo de respuesta de la aplicación.

El modelo tiene tres opciones principales de almacenamiento:

- En un dispositivo lector.
- Remotamente en una base de datos centralizada.
- Sobre un testigo portable.

Con un dispositivo lector, las ventajas se encuentran en el tiempo de respuesta; ya que el usuario no tendría que esperar para que la autenticación o identificación pase sobre otros sistemas o recursos de red, se evitarían los ataques provenientes de orígenes externos y se tendría un control y acceso más fácil.

Pero, ¿qué pasa si la cantidad de usuarios es considerable?; mayor aún, ¿qué pasaría, si muchos usuarios quieren acceder al sistema casi al mismo tiempo?, nos podríamos meter en problemas, esto no lo soportaría un simple dispositivo. Para este tipo de circunstancias o cuando existen múltiples sistemas, es mejor almacenar los modelos

[1] En inglés se le denomina: "template" o "score".

en una base de datos central. Aunque ésta es una mejor opción, se debe tener en cuenta que si el sistema llega a tener fallos o si la información de la base de datos llega a ser corrupta es posible que se tengan que registrar a los usuarios nuevamente. Entonces, una vez implementada la base de datos debemos considerar la seguridad de su resguardo también.

La agregación de recursos y el tráfico de red creados entre la base de datos y el lector biométrico son otras desventajas de este tipo de almacenamiento; por otro lado si la red no está disponible en algún momento, el lector biométrico no sería de utilidad y con todo lo ya mencionado debemos entender que nuestro sistema es más vulnerable ahora, pues contamos con ataques internos y externos.

Por otro lado si almacenamos el modelo en un testigo el usuario tendría la posesión absoluta de sus rasgos. El testigo puede ser usado para diversos dispositivos y/o lectores, haciéndolo más conveniente para las organizaciones; ya que tendrían lectores en diferentes ubicaciones y al usuario final se le puede hacer sentir más cómodo.

Una desventaja es el coste de cada testigo por usuario. Esto puede llegar a ser un gran coste, además de que si el usuario perdiera su testigo, para recuperarlo debemos contar con el tiempo del nuevo registro y el coste del nuevo aparato.

Por otro lado esto corresponde a una gran vulnerabilidad, ya que posiblemente el testigo no fuera usado por la misma persona. Debemos tener en cuenta que nunca debería ser usado para información sensible, confidencial y/o clasificada; increíblemente las leyes en algunos países requieren que la información sea almacenada sobre testigos o en tarjetas inteligentes [Zimmerman02].

La mejor solución a implantar es un sistema con múltiples almacenamientos acorde a las necesidades. Esto permitirá a las organizaciones combinar los beneficios y al mismo tiempo erradicar ciertas desventajas.

3.2.2) Módulo de Identificación y Autenticación

El módulo de identificación o autentificación es la comparación de datos capturados durante el proceso de registro y los datos

biométricos reunidos durante un proceso de solicitud de identificación y/o autenticación. Durante la fase de identificación o autenticación, el sensor biométrico captura las características de la persona a ser identificada o autenticada y las transforma dentro del mismo formato digital que el modelo. El modelo resultante es introducido a la fase de comparación (match stage), en la cual se compara con el modelo almacenado y se determina si los dos modelos coinciden (matching)[2].

El aparato biométrico puede ser fabricado para que actualice las muestras, ya que pueden ocurrir cambios a los rasgos físicos u conductuales como pueden ser cortadas, rasguños, envejecimiento, etc. Por supuesto un mayor cambio a estos rasgos, resultaría en una no identificación o no autenticación y resultaría en un nuevo registro.

Un sistema biométrico lo podemos utilizar para dos objetivos:

- **Identificación.- Determina quien una persona es** [Hay04]. Es una coincidencia uno-a-muchos. Obsérvese que aquí el usuario no suministra su identidad.
- **Autenticación.- Determina si una persona es quien ella dice ser.** Es una coincidencia uno-a-uno. Obsérvese que aquí el usuario si suministra su identidad [Faúndez98].

3.2.2.1) Identificación

En un sistema de reconocimiento, cuando la(s) característica(s) capturada(s) y alguno de los modelos es el mismo, el sistema identifica a la persona con las coincidencias de los modelos. Donde por ejemplo en [Markowitz05], todos los miembros de algún equipo de un proyecto ***tienen la misma palabra clave***, a lo mejor un número de identificación de proyecto; entonces, cuando uno de ellos se presenta para ser identificado, **el sistema debe hacer varias comparaciones** en una base de datos para checar si la persona es un miembro del equipo y determinar que miembro es (Figura 8).

[2] En este punto se puede implantar una política de seguridad sobre el número de intentos que se deseen otorgar para usar la aplicación; es decir, un número razonable de intentos al usuario legítimo por si llega a equivocarse al ingresar sus datos, pero no debe ser un número exagerado de intentos como para comprometer al sistema [13].

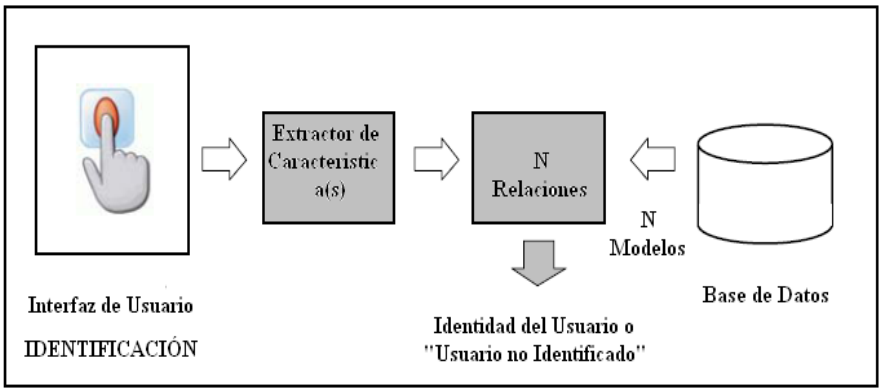


Figura 8.- Procedimiento de Identificación

3.2.2.2) Autenticación

En un sistema de verificación, cuando la(s) característica(s) capturada(s) y el modelo almacenado de la identidad solicitada son el mismo, el sistema concluye que la identidad solicitada es la misma. Por ejemplo, cuando cada uno de los miembros autorizados de un equipo de algún proyecto tienen ***su propia palabra clave,*** en conjunto con algún sistema biométrico por ejemplo la verificación del hablante, **el sistema hace una única comparación** entre la identidad del miembro del equipo y su propia palabra clave por medio del sistema biométrico; con esto se determina la autenticación del usuario (Figura 9).

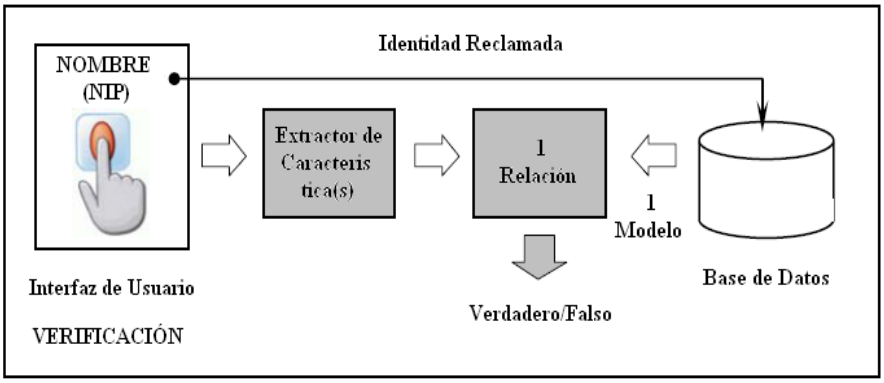


Figura 9.- Procedimiento de Autenticación

Prácticamente los sistemas de identificación se pueden usar de dos maneras:

- Los de identificación positiva que tratan de encontrar al usuario en su base de datos y
- Los de identificación negativa que tratan de asegurar que el usuario no se encuentre en su base de datos.

Para implementaciones públicas de sistemas de seguridad biométrica se tiende más hacia la identificación, mientras que instituciones privadas tienden más hacia la autenticación [Penny02]. Además que se intuye que el módulo de identificación es más lento que el módulo de autenticación porque se requiere mayor procesamiento, pero cuando el número de usuarios es pequeño, estas diferencias se desvanecen.

3.3) TIPOLOGÍA DE LA TECNOLOGÍA BIOMÉTRICA

Hay diferencias importantes entre los métodos fisiológicos y los conductuales. Primero, el grado de variación intra-personal en una característica fisiológica es mucho más pequeña que en una característica conductual. Por ejemplo lesiones fuertes en el ojo pueden no modificar la estructura del iris con el tiempo, mientras que las características del habla cambian y son influenciadas por muchos factores en el tiempo, por ejemplo el estado emocional del hablante. Los desarrolladores basados en sistemas conductuales, por lo tanto, tienen un más duro trabajo en compensar estas variaciones intra-personales.

Segundo, debido a las variaciones intra-personales de los métodos conductuales, su poder discriminatorio ("¿Cómo cuántas personas distinguibles hay?") es generalmente más pequeño que para los métodos fisiológicos [Murray67].

Una de las principales ventajas de muchos sistemas biométricos conductuales es que la detección de una persona viviente es intrínseca y ninguna medida especial necesita ser tomada. Posibles ejemplos incluyen sistemas de reconocimiento de la firma y sistemas de reconocimiento por la manera de caminar, pero no del habla, aunque es una característica conductual muy popular, ella puede ser fácilmente grabada. Sin embargo es obvio que no se pueda robar la firma de alguien removiéndola o cortándola de su mano.

3.3.1) Biometría para analizar y/o reconocer la fisiología de una persona

La biometría física mide muchas características únicas de alguna parte del cuerpo humano para crear una impresión o un modelo. Se dice que este tipo de biometría es más apropiado cuando usamos aplicaciones de seguridad media-a-alta [Cherry04].

La biometría física más común que encontramos incluye técnicas como impresiones dactilares, geometría de la palma o mano, reconocimiento del iris o retina y características faciales. Existen también, técnicas menos usadas como la forma de las orejas, la temperatura corporal (termografía) y la forma del cuerpo, entre otras.

3.3.2) Biometría para analizar y/o reconocer el comportamiento de una persona

Son basadas sobre medidas o datos de acciones de una persona (cosas que nosotros hacemos que son únicas para nosotros). Se dice que este tipo de biometría es suficiente cuando usamos aplicaciones de seguridad baja-a-media; ya que parece ser imposible, pero por ejemplo, se puede replicar el patrón de la firma de un individuo.

Existen técnicas como la firma manuscrita, el reconocimiento de la manera de caminar y el análisis gestual, entre otras.

Podemos ver en la figura 10 una pequeña, pero ejemplificante clasificación de algunos biométricos.

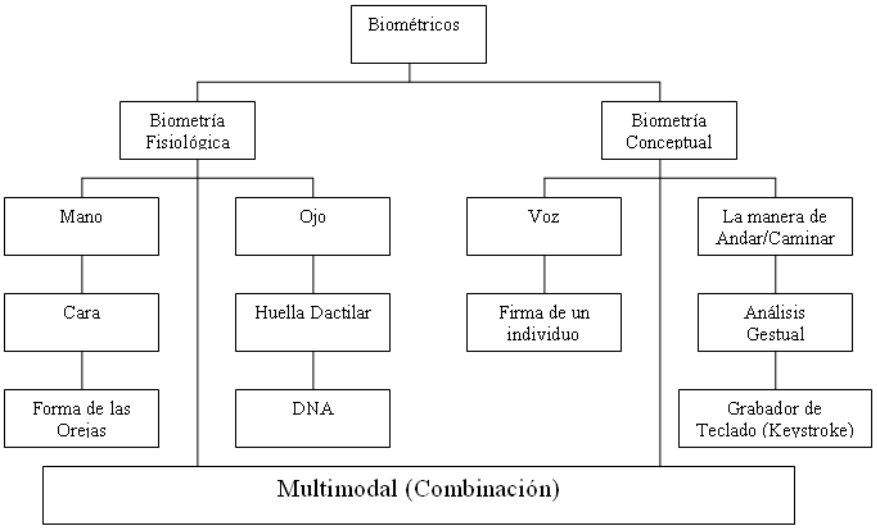


Figura 10.- Tipología en los Métodos Biométricos [Murray67]

3.4) FUNCIONAMIENTO DEL SISTEMA Y CUESTIONES DE DISEÑO

Si la demanda para las aplicaciones de identificación y verificación se encuentra en todas partes y los métodos convencionales para la identificación personal son inadecuados. ¿Por qué, entonces, la

tecnología biométrica no ha sido tan difundida como muchos esperásemos que fuera? Una de las razones fundamentales es el funcionamiento.

Algunas de las cuestiones que caracterizan a un sistema biométrico incluyen: exactitud, precisión, velocidad computacional, coste, facilidad de uso, facilidad de desarrollo, seguridad, integridad y por supuesto un factor interesante, la privacidad.

3.4.1) Exactitud

A diferencia de los demás métodos de autenticación, en la tecnología biométrica, aún si una característica legítima es dada, ***la autenticación correcta no puede ser garantizada.*** Esto puede ser por diferentes cuestiones como el ruido de las señales del sensor (naturales y las propias del mismo aparato extractor de muestras), las limitaciones de los métodos de procesamiento, y aún más importante, la variabilidad de las características físicas o conductuales, además de su presentación.

La *tasa de fallas de captura* nos da el porcentaje de veces que el dispositivo biométrico falla para capturar una muestra cuando las características son presentadas a éste. Este error típicamente ocurre cuando el dispositivo no es capaz para ubicar una señal biométrica de suficiente calidad [Jain04].

Algunos suplantadores causan estas fallas deliberadamente, buscando que se les otorguen privilegios fuera del sistema (Ver figura 11).

Como se puede apreciar, este par de señales son las mismas, pero la posición en que se extrajeron, no.

Figura 11.- Huella Dactilar desde dos posiciones distintas

Con lo ya mencionado, podemos decir que ***dos modelos del mismo sistema biométrico no coincidirán al 100% las características, el 100% de las veces.*** La confiabilidad y la calidad del escaneo causarán la variabilidad del resultado.

3.4.2) Precisión

La principal y más crítica característica de los sistemas de identificación/autenticación biométricos es su precisión. Si el sistema no puede separar con precisión a los usuarios de los impostores, en realidad no es un sistema de identificación o autenticación. Los dos elementos que permiten medir la precisión son la tasa de falsos rechazos y la tasa de aceptaciones equivocadas. Donde la *tasa de error equiprobable (*o *Crossover Error Rate* en inglés) es la principal medida de precisión en un sistema biométrico.

Todos los fabricantes deben permitir ajustar algunos parámetros para optimizar el rendimiento del sistema, de acuerdo a las necesidades del usuario. Entre estos parámetros se encuentran las tasas de errores; donde el ajuste de los sistemas se hace en la práctica cambiando el umbral de aceptación o de rechazo.

Puesto que no es frecuente que el identificador o la herramienta de autenticación del usuario coincidan exactamente con su registro, hay que aceptar que algunos valores del identificador o del dato que autentica sean distintos. El umbral es una especificación de cuantos valores pueden diferir y por cuánto. Así se puede ajustar el umbral para que aumente el número de aceptaciones equivocadas (menos seguridad en el sistema) pero menos rechazos falsos (más amigable al usuario). Y cuando ambos valores son iguales se tiene la tasa de error equiprobable, la cual se muestra a continuación.

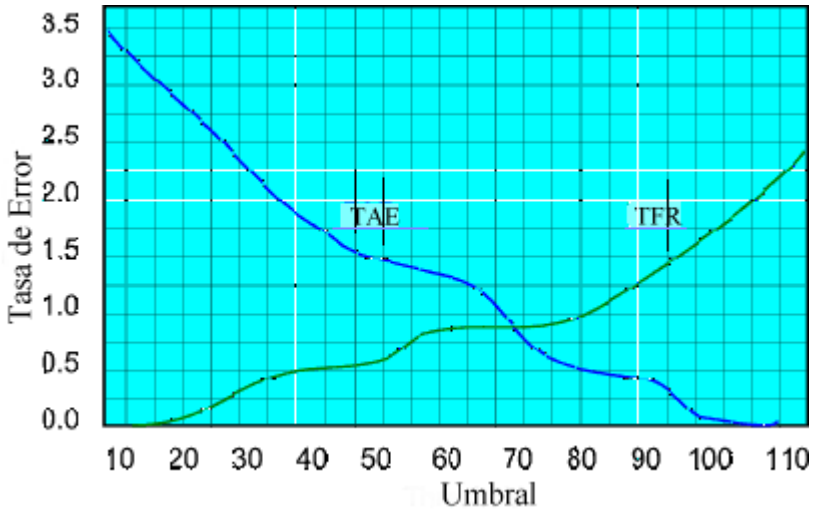


Figura 12.- Umbral de las Tasas de Error

Cuando un sistema alcanza un extremo, se aleja del otro. Pero los sistemas solo pueden funcionar en una sola configuración. La tasa de error equiprobable (TEE) que es una métrica justa para cualquier sistema pues toma en cuenta ambas características. Un sistema que ofrezca una TEE de 2% será en general más preciso que otro que tenga una TEE del 5% pues es igualmente probable un rechazo falso que una aceptación equivocada, y la probabilidad de ambas es el porcentaje que se menciona.

Las cifras que menciona el fabricante pueden diferir de la realidad; ya que, tienden a ser las obtenidas en condiciones ideales en las instalaciones del fabricante. Así que el funcionamiento óptimo de un sistema depende de cómo se use.

Usuarios mal capacitados o procedimientos de registro con baja calidad afectarán los resultados. Quizás, dada la creciente importancia de este campo algunos países establezcan centros nacionales de medición de sistemas biométricos.

3.4.2.1) Tasa de Aceptaciones Equivocadas

La tasa de aceptaciones equivocadas (TAE) es el porcentaje de impostores que son aceptados. Estos errores son los que se consideran más graves en sistemas biométricos, pues permiten el acceso a intrusos o suplantadores. La biometría basada en rasgos fisiológicos tiene un índice más alto de TAE.

Si la precisión es baja, el riesgo en que una muestra inválida sea aceptada, será más alto.

El porcentaje de aceptaciones equivocadas lo podemos medir con la siguiente fórmula:

TAE = IA/I * 100%

Donde IA es el número de impostores aceptados e I es el número de impostores que reclaman esa identidad.

3.4.2.2) Tasa de Rechazos Falsos

La tasa de rechazos falsos (TRF) es el porcentaje de usuarios válidos, que son rechazados por error. La biometría basada en el comportamiento tiene un índice más alto de TRF [Zeg02].
Los falsos rechazos causan descontento en los usuarios legítimos, y pueden significar pérdidas para un negocio que emplee un sistema poco preciso. Muchas instituciones que usan sistemas biométricos están dispuestas a aceptar unas cuantas aceptaciones equivocadas mientras no se hagan rechazos falsos.

El porcentaje de rechazos falsos lo podemos medir con la siguiente fórmula:

$$TRF = CR/C * 100\%$$

Donde CR es el número de clientes rechazados y C es el número de usuarios que reclaman su identidad [Ben-Yacoub99].

Es importante encontrar un balance correcto entre la aceptación equivocada y los rechazos falsos. *El sistema debe proveer un suficiente nivel de seguridad, también como proveer el uso y la aceptación del usuario.*

Generalmente si las TRF son mayores, se utilizan más para aplicaciones de seguridad; mientras que si son más altas las TAE se utilizan más para aplicaciones forenses y un balance entre ambas, es utilizado para aplicaciones civiles.

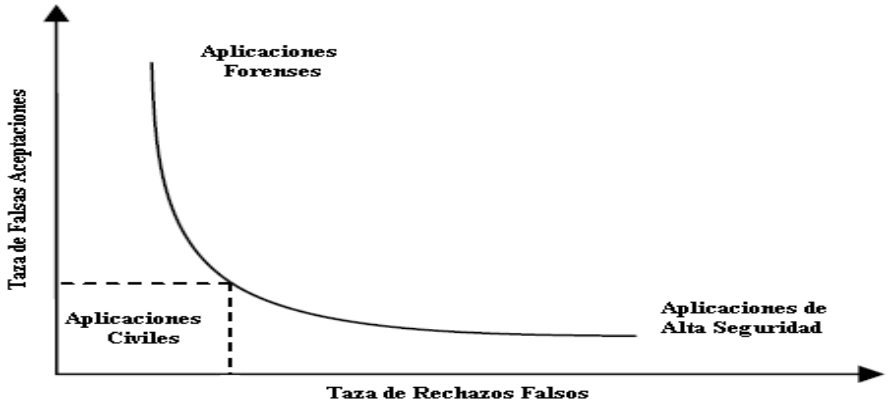


Figura 13.- Aplicaciones respecto a las Tasas de Error

3.4.2.3) Precisión para Identificación y para Autenticación

Como sabemos debe existir la tasa de error sobre cualquier biométrico, pero ¿éstas serán las mismas si aumenta el número de usuarios sobre nuestro sistema?

Sobre la autenticación no hay variación alguna; ya que, siempre contaremos con un solo usuario; pero, ¿qué pasa cuando la base de datos va creciendo?, ¿se tendrán las mismas tasas de error para un sistema que contiene a 1 usuario que otro sistema que contiene a 1000 usuarios?

La respuesta es que las tasas de error van aumentando respecto a mayor número de usuarios sobre el sistema. Para eso contamos con la siguiente fórmula [O´Gorman04]:

$$Total(n) = 1 - [1 - TFR(1)]^n$$

Donde

TFR = La tasa que indica falsos rechazos (Por ejemplo para el iris 1 – 131 000 ó .000131)
n = Número total de usuarios sobre el sistema

Para usarla como autenticación biométrica tendríamos lo siguiente:

$Total(n) = 1 – [1 - TFR(1)]^n$ donde

$Total(1) = 1 – [1 - .000\ 131(1)]\wedge 1$ =
$Total(1) = 1 – [1 - .000\ 131]\ \wedge 1$ =
$Total(1) = 1 – .999869$ = .000131

O que es lo mismo 1 error en cada 131 000 usuarios.

Pero para usarla como identificación biométrica en una base de datos de 1000 personas, tendríamos lo siguiente:

$$Total(1000) = 1 - [1 - .000\ 131]^{\wedge 1000} = .122789$$

O que es lo mismo 1 error en cada 122789 usuarios.

Como podemos ver, nuestras estadísticas varían respecto al número de usuarios que están contemplados en nuestro sistema; en el ejemplo mencionado no parece ser que varíe mucho, pero, ¿qué pasaría si utilizáramos un biométrico de huella dactilar en una base de datos sobre 100 personas?, donde la tasa de falsos rechazos para la huella dactilar es de $1 - 500$[3].

Con esto podemos deducir que entre más grande sea el número de entradas en sistemas basados en identificación, es mayor la posibilidad de falsos rechazos o falsos aceptados [Penny02], entonces, aquí tenemos otro punto clave al momento de analizar una tecnología biométrica, además de que la relación uno-a-muchos no siempre es la más adecuada, y lo mejor sería implantar una solución 1-a-pocos [O´Gorman04].

3.4.3) Velocidad Computacional

La rapidez y la tasa de operación son también características importantes, no para la autenticación o identificación sino para el usuario final. La rapidez depende el sistema de cómputo y del sensor que indica el tiempo necesario para anunciar una decisión. La tasa de operación se mide desde que el usuario se acerca al sensor hasta que el usuario logra acceder al sistema. Se considera que una rapidez de 5 segundos es aceptable. Tasas de operación de 6 a 10 usuarios por minuto (o sea de 10 a 6 segundos por usuario) son razonables.

Además que haciendo un mecanismo multi-factor [Bolle03] únicamente con un sistema biométrico se reduce el problema de coincidencias uno-a-muchos (reconocimiento) a coincidencias uno-a-uno (verificación). La verificación no gasta tanto tiempo de procesamiento y recursos de cómputo como la identificación; ya que no necesita comparar la muestra viva a la entrada de la base de datos hasta que encuentre una coincidencia.

[3] Muchas de las aplicaciones actuales son implantadas bajo este esquema, incluso bancos.

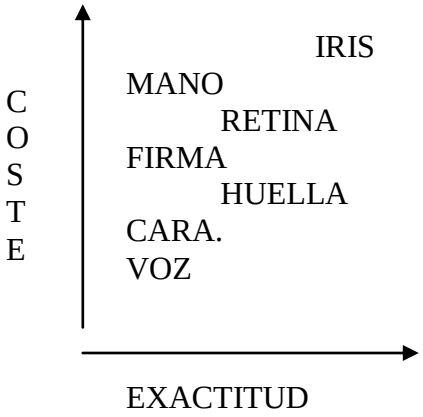
3.4.4) Coste

Otro aspecto importante antes de implantar una tecnología, es ver si va a ser *factible*; es decir, que el coste de implementación de la tecnología biométrica (TB) no deba ser más costoso en un determinado tiempo (T), que el valor de los activos (A), o sea:

$$A > TB * T$$

Ya que si esto no es llevado así, la tecnología biométrica sobrepasaría el valor de los activos, obteniendo pérdidas en vez de beneficios.

El coste está muy ligado con la exactitud. Muchas aplicaciones como entrar al sistema de una computadora son sensibles al coste adicional de incluir tecnología biométrica.



Las tecnologías más costosas no necesariamente son las más exactas

Con la disponibilidad de producción a gran escala de sensores baratos, se contribuirá para hacer accesible a los sistemas biométricos a nuevas aplicaciones de identificación y autenticación personal; además de que incrementando el uso de los sensores se pueden llegar a tener precios aún más bajos.

En algunas aplicaciones como en computadoras portátiles no se pueden incorporar grandes sensores biométricos por hardware, esto deberá impulsar el desarrollo de la miniaturización de sensores.

3.4.5) Facilidad de uso

La facilidad de uso en un sistema biométrico recae considerablemente con la cooperación del usuario; ya que es un aspecto realmente decisivo para aplicar una tecnología biométrica.

La adquisición de las muestras se dice que es desde incómoda hasta fastidiosa; muchas veces esto tiene que ver con la ignorancia del usuario; otras más por cuestiones de salud; y otras más, miedo a las posibles violaciones a la privacidad.
La única manera en que el usuario acepte dicha tecnología es basándose en la comprensión del funcionamiento del sistema y no queda más que combatirla con capacitación (aunque ésta en algunas ocasiones es tardada) y comprensión.

Argumentos que no tienen más fuerza que la psicología[4], nos ayudarían con algunos impedimentos como el de la salud al decir que; tratándose de técnicas que no invadan al cuerpo humano, y de análisis matemáticos de características que están a la vista de todos, no pueden causar daño alguno, como en el caso de la manera de caminar; ya que muchos de los sensores son cámaras.

3.4.6) Facilidad de desarrollo

La tecnología biométrica necesita hacer el acceso fácil para la integración de sistemas y la implementación. Esto en nuestros días no ha sido posible por su escasez en estándares.

Mientras nosotros estamos lejos de una simple uniformidad de datos y estándares API para todas las tecnologías biométricas, los esfuerzos ya están en camino.

3.4.7) Seguridad

El cual refleja que tan fácil el sistema puede ser burlado usando métodos fraudulentos [Jain04].

[4] Ashbourn a hecho considerables investigaciones en esta área y provee muchos detalles en su documento que se puede ver en la liga http://homepage.ntlworld.com/avanti por si se quiere profundizar en el tema [22].

3.4.8) Integridad

La identificación o verificación no sirven de nada si el sistema no puede proveer la legitimidad del propietario que presenta las muestras. Entonces una quinta tasa encontrada es la *Tasa de Fallos al Momento del Registro.* Esta tasa es el registro de los usuarios dentro del sistema que no es satisfactoria [Myers02], debido a que posiblemente no se tengan las características necesarias y suficientes para realizar el registro.

Por ejemplo, en alguna fracción de cierta población, se puede o no poseer una biometría particular o se puede presentar una característica que no presente alguna información útil, como lo que se verá a continuación en la figura 14:

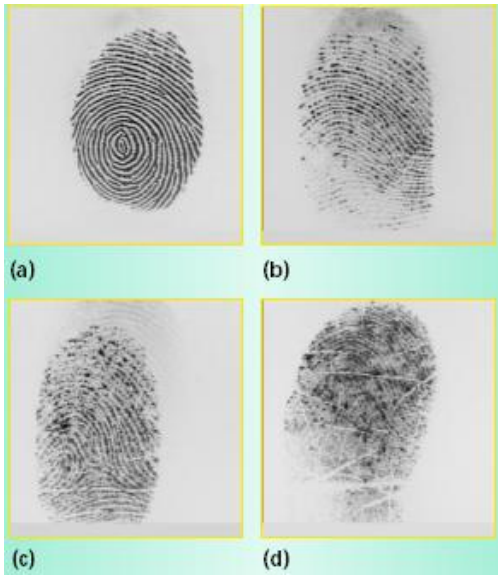


Figura 14.- Huellas Dactilares (Cortesía de la Academia de Kluwer)

La información en (a) es útil, en (d) no lo es y en (b) y (c) es mínima.

Además, que, estas huellas tomadas del dedo pulgar, puede que no todas las personas cuenten con dicho dedo.

Para aplicar exitosamente una tecnología biométrica para una aplicación de identificación o autenticación personal, es importante entender y realmente evaluar la tecnología en el contexto de una aplicación y población establecidas.

Para terminar este capítulo haré mención de dos ejemplos que ilustran algunas consideraciones que se deben llevar a cabo para establecer una tecnología biométrica y al final mencionaré ciertas cuestiones de privacidad que se deben también tomar en cuenta.

Ejemplo de una *aplicación*:

Basándome en [Dunker04], el reconocimiento del hablante está en los más altos rangos en la aceptación del usuario, es más fácil de usar y menos caro que el reconocimiento del iris, pero...

El reconocimiento del hablante tiene una tasa de error 1-en-50, y el reconocimiento del iris 1-en-131,000. Los falsos rechazos son fáciles de producir para el reconocimiento del hablante, y los errores pueden ocurrir debido a ruido y/o resfriados. El reconocimiento del hablante puede ser usado para verificar la identidad de una persona, pero no es recomendado para su identificación. El reconocimiento del iris es recomendado para ambos: identificación y autenticación.

Como vemos aquí, al momento de tratar de implantar una tecnología biométrica, se debe de hacer un análisis minucioso sobre la biometría que se desee aplicar; aspectos como la tasa de error son importantes; ya que con ésta se puede deducir ***hasta cuantos miembros soportaría nuestra aplicación***; ya sea para identificación, autenticación o ambas.

Otro aspecto importante es el tipo de aplicación a usar ¿Cuál es la biometría adecuada para la circunstancia adecuada? es decir; antes de implementar una tecnología biométrica, se tiene que hacer un estudio sobre qué biometría es la que mejor satisface las necesidades del usuario. Algunas de las cuestiones que intervienen, son el nivel de seguridad deseado y la aceptación de los usuarios.

Ejemplo de una *población establecida*:

Concentrémonos en las religiones. En el mapa de la figura 15 observamos que la religión islámica tiene una gran difusión a nivel mundial.

Figura 15.- Religiones en el mundo

En ésta religión, las mujeres tienen ciertas restricciones. Entre una de ellas está la forma de vestir (Figura 16).

Figura 16.- Mujeres musulmanas

Anteriormente las mujeres musulmanas se cubrían el rostro con un velo semi-transparente de media cara, conocido con el nombre de *hijab*. Ahora debido a cambiantes restricciones en la religión, deben usar túnicas negras llamadas *abaya*. Éstas deben ser portadas en cualquier lugar público sin importar el calor que tengan que soportar, las cuales sirven para taparse la cabeza, el rostro y el cuerpo, incluyendo las manos.

Como vemos aquí, al momento de tratar de hacer una implementación biométrica se debe de hacer un análisis del ambiente en el cual se va a implementar una cierta tecnología biométrica; ya que, en poblaciones donde haya mujeres musulmanas, debido a las restricciones de su religión, países como Arabia Saudita, Irán, Egipto, Argelia, Libia, etc. no se podría implementar ciertas biometrías como el reconocimiento de cara, manos, morfología de la oreja, entre otros.

Podemos decir que, *la certeza de una implementación de una biometría dada es sensible a una población fija;* ya que, ciertas biometrías pueden no ser aceptados en ciertos segmentos de alguna población fija.

Con esto concluimos que ninguna biometría reúne efectivamente todos los requerimientos de todas las aplicaciones. En otras palabras; ningún simple biométrico es "optimo". La relación de una biometría y una aplicación dada, es determinada sobre el modo de operación de la aplicación y las propiedades de las características o rasgos [Jain04].

3.4.9) Privacidad

Hay algunos preconceptos negativos e incluso para algunas personas pueden ser los más significativos en cuestión a la implementación de un sistema biométrico. Preguntas como: ¿Los datos biométricos pueden ser utilizados para rastrear a las personas? ¿Secretamente se pueden violar los derechos a la privacidad? Hay una gran diferencia entre los términos percepción y realidad; ya que el sistema puede hacer percibir al usuario que el sistema nos proporciona *únicamente* los resultados que nosotros esperásemos ver, mientras que por otro lado ese mismo sistema, puede ser manipulado con otros fines, aparte del deseado.

Cabe señalar que el objetivo de la biometría únicamente pretende identificar quienes somos, en la mayoría de los casos buscando nuestra propia protección y seguridad, pero esto por otro lado, parece ser un cierto atentado contra la intimidad personal [Faúndez98].

Muchas personas en el ámbito de la autenticación por sistemas biométricos están preocupadas por la información personal que puede ser explotada de manera ilícita con fines fuera del objetivo de la aplicación. Esto es conocido como *invasión a la privacidad*.

Los usuarios tienen el derecho de saber, por ejemplo, como sus datos serán usados y quién tendrá acceso a ellos.

Hay una herramienta en Internet denominada Biometric User´s Charter la cual ayuda a reunir información valiosa que debe conocer

tanto el usuario como el proveedor del servicio con el objetivo de obtener mejores soluciones biométricas[5].

Parte de la información que debe conocer el usuario acerca de sus datos es la siguiente:

- Naturaleza de los datos para ser mantenidos
- Almacenamiento de los datos
- Seguridad de los datos
- Acceso a los datos
- Administración de los datos
- Derechos del usuario en consideración a los datos

El buen uso de esta información ayudará a los usuarios para hacer las preguntas correctas antes de que se registren ante el sistema y los proveedores por su parte deberían aliviar las preocupaciones de los usuarios difundiendo como operan sus sistemas [Penny02]. Con esto se logra crear conciencia sobre este tema poco difundido y los resultados que se obtendrán serán la seguridad en la industria biométrica en la construcción de una implantación de una estructura ética para la confidencialidad del usuario.

Hay que recordar que una fuerte seguridad es basada en la ciencia y las matemáticas; estas ventajas deben de ser siempre medidas en contra de los riesgos del robo de identidad y el fraude.

Por lo tanto, la diferencia radica en cómo esta tecnología será usada. Para el propósito de autenticar a un individuo, el sistema no debe de determinar la identidad del usuario, *sino solamente debe confirmarla*. Para los propósitos de autenticación, los datos almacenados deben de encontrarse como una representación matemática que no pueda recrear la imagen original [Zimmerman02].

Es por eso que el director ejecutivo de IBIA (International Biometric Industry Association), Richard E. Norton cita algunos contratiempos, en los que se encuentra la implementación de los sistemas biométricos y las maneras en que esos mitos pueden ser erradicados (Tabla 6) [Lewis02].

[5] Se puede descargar desde: http://homepage.ntlworld.com/avanti/

MITO	HECHO
Invasión de la privacidad	Únicamente revisan la información que es necesaria, sin invadir la privacidad.
Los datos resguardados indican quien tú eres	Únicamente la muestra aislada, no revela nada acerca del portador.
Los datos pueden ser usados para robo de identidad	Las muestras son dinámicas; una exacta coincidencia indicaría fraude.
Puede ser usado para enlazar información de varios orígenes	Las diferencias entre modelos previenen de comparaciones registro a registro.
Los datos pueden ser interceptados y usados para hacer fraude	No se puede usar ingeniería inversa para simular una lectura viva.
La información transmitida por la red es vulnerable	PKI y tecnologías de cifrado biométrico aseguran la transmisión de los datos.
Los datos almacenados en una base de datos son una amenaza	Se regula por medio del uso de las soluciones manejadas por base de datos.
Te pueden rastrear en donde quiera que vayas	Imponen una significante barrera en contra del rastreo.
La tecnología de vigilancia no es constitucional	Suprema Corte de E.U.A.: No es razonable esperar privacidad en un lugar público.

Tabla 6.- Miedos en la Biometría (Crédito: R. E. Norton, IBIA, 2002)

Hoy en día la gran demanda de móviles individuales, y las comunicaciones remotas, han traído como resultado la rápida entrega en el mercado de servicios baratos; sin tomar la debida importancia a la seguridad personal; cada vez llega a ser más difícil y cada vez existe un crecimiento mayor de fraude en nuestra sociedad [Pankanti00].

Lamentablemente los sistemas biométricos han tenido pobres estudios respecto a la autenticación biométrica y sus consecuencias. La implementación hoy en día de esta tecnología puede ser catastrófica, por lo anteriormente ya citado.

IBIA se encarga de legislar y regular a la biometría de manera que impida el robo de identidad e incremente la seguridad personal.

La IBIA recomienda:

- Salvaguardar los datos del sistema biométrico para garantizar que no sean mal usados y no comprometan algún tipo de información.
- Políticas que claramente establezcan como los datos biométricos serán recolectados, almacenados, accedidos y usados.

- Condiciones limitadas sobre cuales agencias de seguridad nacional y refuerzos de leyes puedan adquirir, acceder, almacenar y usar datos biométricos; y
- Controles para proteger la confidencialidad y la integridad de las bases de datos conteniendo datos.

Hemos encontrado un gran reto para la industria, el medio y la academia en la investigación a este tema; incluso, deben de ser puntos estratégicos de un estándar saliente. La IBIA está abierta para fabricantes, integradores y usuarios, su página es la siguiente: http://www.ibia.org.

Es peligroso evitar ciertas tecnologías por miedo a que sean usadas injustamente. Lo mejor es tratar de investigar las tecnologías a fondo, para poder afinar los sistemas, por ejemplo al tratar de hacer un estándar con un alcance lo suficientemente maduro para evitar abusos y/o errores al momento de implantar una nueva tecnología.

Con esto podemos entender cada vez más la necesidad de analizar y modelar una tecnología biométrica en un escenario específico. Es por eso que no se puede dar un instructivo secuencial de los pasos a seguir para implementar cierta tecnología biométrica, en nuestro caso la autenticación del caminante.

Una manera concreta de decir que la tecnología biométrica asegurará cierta autenticación ya se vio que no es posible, lo que sí se puede hacer es estudiar a fondo cierta tecnología biométrica para saber cómo atacar el problema y saber que se tiene que hacer para implementarla y solo así para obtener los resultados esperados. Es por eso que el siguiente capítulo muestra a detalle la tecnología biométrica por la manera de caminar de las personas esperando dar al lector el discernimiento esperado y la respuesta a la pregunta: ¿Es posible implementar la autenticación biométrica por la manera de caminar de las personas?

¿Cuál es la probabilidad de que dos maneras de caminar sean iguales?

"Green R. y Guan L."

IV BIOMETRÍA POR LA MANERA DE CAMINAR DE LAS PERSONAS

4.1) ESTUDIO DEL CAMINAR HUMANO

4.1.1) Antecedentes en la investigación por la manera de andar

La manera de andar no es un nuevo tema de estudio o literatura científica. Ha sido investigada y examinada en varios aspectos sobre décadas pasadas. Estudios médicos como el Parkinson [Schmidt00], estudios referentes a la industria del calzado en tenis, en matemáticas, modelado del cuerpo humano [Nixon99] y en psicología han sido llevados a cabo y en los cuales se comenta que la manera de andar puede comportarse como una característica única. Por su parte Aristóteles y Leonardo da Vinci estudiaron el movimiento del cuerpo humano y en literatura podemos mencionar a Shakespeare quien redactó tempranas citas refiriéndose a la posibilidad del reconocimiento por la manera de andar [Yam01].

Murray en 1967 [Murray67] realizó un estudio para caracterizar patrones de movimiento en varias partes del cuerpo humano que se forman en el momento en que una persona se encuentra caminando. Obtuvo patrones específicos como puntos de referencia los cuales iluminó con luz estroboscópica mostrándola 20 veces por segundo.

El resultado obtenido fue que la manera de caminar puede ser tomada como una característica única personal, pues cita que si todos los movimientos al momento en que una persona se encuentra caminando (24 puntos diferentes según estudios médicos [Murray67] y [Murray64]) fuesen considerados, la manera de caminar podría ser usada como una prometedora característica para la identificación humana.

Estos tempranos resultados fueron alentadores y prometedores, pero la manera de caminar no había sido propuesta como una característica biométrica hasta hace poco. Posibles razones pudieron ser la carencia de confiables y baratos sensores y el insuficiente procesamiento en el amplio volumen de datos. Comparada con otros biométricos como el de cara y el de huella dactilar, el reconocimiento por la manera de caminar se encuentra en su infancia [Wang02], es por esto, que la tecnología biométrica por la manera de caminar no es conocida en su totalidad.

Hoy en día la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA) ha asignado a los investigadores en la visión del cómputo en la UMIACS (University of Meryland Institute for Advanced Computer Studies) para realizar investigaciones en los próximos años con el propósito de desarrollar algoritmos para la identificación de humanos a distancia (entre 50 y 100 pies).

Solamente las continuas investigaciones y desarrollos confirmarán si la biometría por la manera de caminar puede llegar a ser tan funcional como otros biométricos y si sus ventajas de aplicación realmente lo podrían hacer una elección pragmática [Nixon99].

4.1.2) El movimiento humano como manera de andar

Definamos a la manera de andar como una coordinada, combinación cíclica del movimiento humano que resulta del traslado de un lugar a otro [Boyd05]. Los movimientos son coordinados en el sentido de que ellos deben ocurrir como un patrón específico temporal; además de que deben ser repetidos alternando ambos pies. La naturaleza de ambos movimientos generando un traslado, hace a la manera de andar de una persona una característica única.

Ejemplos de la manera de andar de un individuo pueden ser: *el caminar, el correr, el trotar y el escalar.*

Sentarse, recoger un objeto o arrojarlo son todos movimientos coordinados, pero no son cíclicos. Los saltos con palmadas son movimientos coordinados y cíclicos, pero ellos no resultan en un movimiento de traslado.

4.1.3) El movimiento humano como manera de caminar

En el mejor de los casos, desde que un infante da sus primeros pasos y hasta que la lejanía en el espectro del tiempo va originando anormalidades en la manera del caminar, se puede contar con la propiedad de medir las características de un caminante. Los desordenes en la manera de caminar en la vejez son frecuentemente heterogéneos y muchas veces recaen en un origen multi-factor.

Dos capacidades son esenciales para el caminar. Primero, la capacidad para mantener *el equilibrio* y el segundo *el movimiento* (locomotion), que es la capacidad para iniciar y mantener un movimiento de pasos rítmico. Aunque estas dos capacidades son esenciales, hay muchos factores que contribuyen al caminar de un individuo, como lo es el sistema esquelético con sus uniones y el sistema neuromuscular.

La manera normal del caminar se rige por la postura y el balance, las cuales requieren precisas entradas de la función propioceptiva (sentido de la posición), la función vestibular (mecanismos del oído interno y sus conexiones con el tallo cerebral), el sentido visual, el auditivo y la información táctil (Ver Figura 17).

Dos de los tres mayores sistemas aferentes (propioceptiva, vestibular y visual) deben ser intactos para mantener el balanceo. Los datos aferentes deben ser integrados en el tallo cerebral y el cerebro a través del motor (piramidal y extrapiramidal) y el camino cerebelar, el cual entonces sirve como arco eferente de la importante habilidad al estar caminando. Disfunciones en los sistemas aferentes y eferentes o en la integración central pueden conducir a problemas en la manera del caminar. La función del sistema extrapiramidal es modular la postura, correctas reacciones y movimientos asociados.

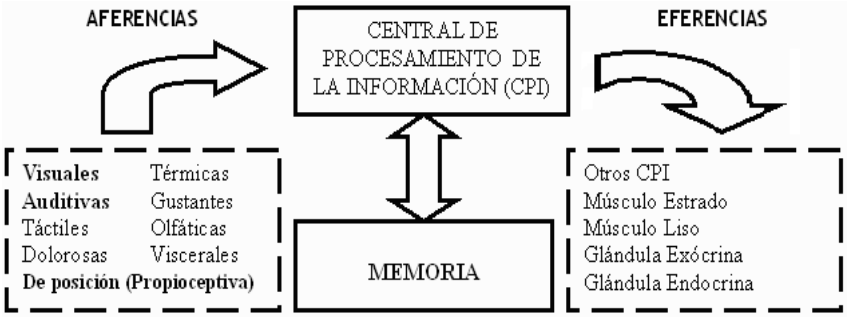


Figura 17.- Modelo de entrada y salida del Sistema Nervioso

4.1.4) El ciclo en la manera de caminar

La definición *de un ciclo en la manera del caminar* es el tiempo en que se presentan dos eventos iguales cuando una persona se encuentra caminando. El pie de cada individuo en un ciclo puede ser dividido en dos periodos: la *postura* y el *balanceo*. Aproximadamente el 60 % del tiempo en un ciclo el pie se encuentra en el periodo de postura y en contacto con la tierra. El tiempo restante del ciclo constituye el periodo de balanceo, donde el pie se encuentra en el aire. El periodo de *doble soporte,* donde ambos pies

están en contacto con el piso y ocurre dos veces en el ciclo. En contraste con el *simple soporte* que es el periodo de tiempo donde solamente un pie está en contacto con la tierra.

El ciclo en la manera de caminar puede además ser desglosado dentro de 8 sub-fases, explicadas a continuación tomando como referencia la pierna derecha (Ver figura 18).

1. *Contacto Inicial*.- El momento en el que el pie derecho, normalmente con el talón, toca el piso.
2. *Reacción de Carga*.- La fase de doble soporte, donde el peso del cuerpo es transferido de la pierna izquierda a la derecha.
3. *Postura Media*.- La primera mitad del soporte del miembro derecho que comienza con el impulso del pie izquierdo y continúa hasta que el peso del pie izquierdo es alineado sobre el soporte del pie derecho.
4. *Postura Terminal*.- Empieza cuando el talón derecho se eleva y continúa hasta que el talón del pie izquierdo toca la tierra.
5. *Pre-balanceo*.- Esta es la segunda fase de doble soporte en el ciclo, que empieza con el contacto inicial del pie izquierdo y finaliza hasta donde los dedos del pie derecho llegan a tocar el piso.
6. *Balanceo Inicial*.- Empieza cuando el pie derecho es impulsado y finaliza cuando el balanceo del pie derecho es opuesto a la postura del pie.
7. *Balanceo Medio*.- Sigue la fase del balanceo inicial hasta que el balanceo de la pierna derecha está enfrente del cuerpo y la pierna inferior es vertical.
8. *Balanceo Terminal*.- Empieza cuando la pierna inferior es vertical y finaliza cuando el pie, normalmente el talón, toca el piso.

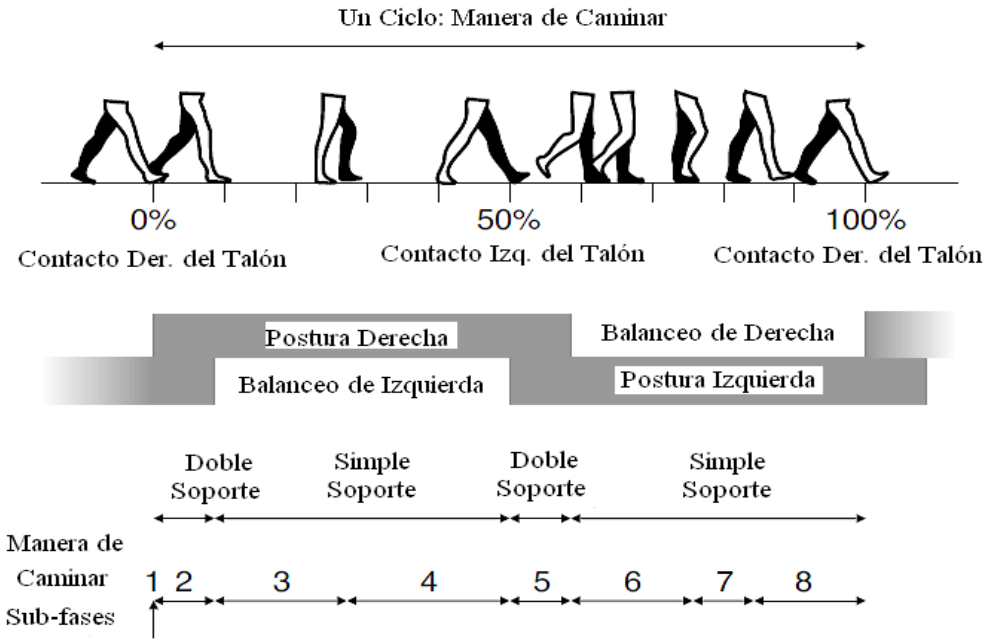


Figura 18.- Diagrama mostrando las diferentes fases del ciclo de un caminante

Los movimientos entre un ciclo consisten de los movimientos de las diferentes partes del cuerpo tales como la cabeza, manos, piernas, etc. Las características de un individuo son reflejadas no solamente en la dinámica y en la periodicidad de un ciclo, sino también por su altura y peso del individuo.

4.1.5) Dynemes

Un reciente paradigma ha sido propuesto como un alfabeto y vocabulario del movimiento humano para cuantificar y reconocer las habilidades de una persona al caminar. *Los dynemes*.

El reconocimiento del cuerpo completo en el movimiento humano nunca ha sido claramente definido en el contexto de la visión del cómputo. Las personas están ejecutando continuas secuencias de movimientos y gestos al caminar, y por lo tanto reconocer específicas habilidades entre el laberinto de uniones de ángulos del movimiento continuo humano es desafiante.

El inicio y fin de cada una de estas habilidades necesita ser localizada. Para esto se requiere la segmentación temporal del movimiento continuo (*CHMR – Continuous Human Movement Recognition*) dentro de dynemes y una metodología para el reconocimiento de un potencialmente ilimitado número de éstas; ya

que hay una natural granularidad de movimientos humanos desde los cuales todos los movimientos humanos son compuestos.

Claramente definiendo estos gránulos o dynemes ayudaremos a desarrollar una visión del cómputo basándonos en un alfabeto y vocabulario de los mismos movimientos humanos.

4.2) ANÁLISIS EN DIFERENTES MÉTODOS DEL RECONOCIMIENTO HUMANO POR LA MANERA DE CAMINAR

Esta tesis se enfoca en la manera de caminar de un humano como el estudio mediante el cual por lo menos un pie se encuentra siempre en contacto con el piso y el estudio se concentra en sus diferentes facetas al caminar [Green06].

4.2.1) Percepción humana por la manera de caminar

Parece que hay una especial conexión entre la manera de caminar de los humanos y la percepción humana. Cohen y otros [Cohen00] observaron que mientras los humanos pueden reconocer fácilmente los movimientos de los humanos, existe la dificultad de reconocer los movimientos de otros animales. Ellos explican que los humanos perciben la manera de caminar de otros humanos por su percepción propia de su manera de caminar. Si esto es correcto, se puede indicar como mejorar la percepción de las máquinas al momento de analizar la manera de caminar de los individuos.

Johansson [Johansson73, Johansson75] demostró que los humanos pueden identificar rápidamente (en menos de un segundo) que un patrón de luces en movimiento (PLM ó MLD por sus siglas en inglés Moving Light Display) pertenecen a un humano caminando; sin embargo, cuando se presenta una única estampa, es casi imposible reconocer la representación de la imagen (Ver figura 19).

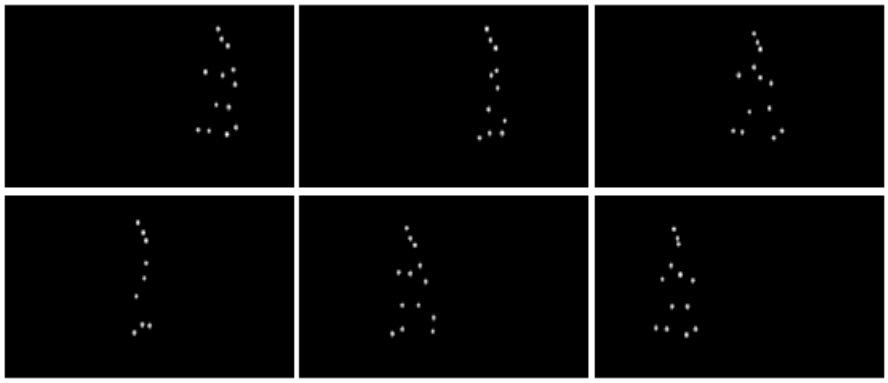


Figura 19.- Cuadros de un PLM de una persona caminando. Las personas pueden identificar rápidamente que la secuencia de los cuadros se refiere al caminar de una persona, pero sería difícil percibirla mostrando un solo cuadro

Investigaciones de Kozlowski y Cutting [Cutting97] y Barclay y otros [Barclay78] mostraron además, que los humanos pueden reconocer también el género de un caminante desde un PLM. Pero lo que parece ser una tarea fácil en los humanos no necesariamente tiene que ser para las computadoras [Murray67].

Como hemos visto, la capacidad de reconocimiento por la manera de caminar ha sido confirmada mediante PLM, pero su capacidad de reconocimiento es limitada. Veamos lo siguiente:

En exposiciones cortas de 2 segundos o menos de un PLM, los humanos no son mejores que un proceso aleatorio. Se requieren más de 4 segundos para que un humano pueda interpretar mejor un reconocimiento a un proceso aleatorio. Aún con esto, la tasa del reconocimiento humano es del 66%, cuando la de un proceso aleatorio es del 50%.

Cutting y Kozlowski [Cutting77] hicieron un experimento que consistía de 6 estudiantes que se conocían entre sí. Se grabaron PLM para cada uno de ellos y se invitó a un séptimo quien los conocía a todos. Esta persona trató de reconocerlos por medio de los PLM. La tasa de reconocimiento fue del 38%, mucho mejor que la de un proceso aleatorio (17%).

La conclusión es que las personas pueden reconocer a sus amigos, pero no lo suficientemente como para ser una confiable forma de identificación. Parece ser que el reconocimiento entre personas recae en otros puntos clave.

Lo que nos queda es seguir analizando métodos nuevos y/o complementarios para obtener resultados más fidedignos para una mejor identificación humana.

4.2.2) Frecuencia de Relación de Fases, Fase de Cierre y Plausibilidad Física

Como la manera de caminar es rítmica y naturalmente es un comportamiento oscilatorio [Stewart99], se puede asumir que éste oscilador natural controla cada una de las extremidades y este movimiento de extremidades puede ser interconectado o asociado de alguna manera.

Bertenthal y Pinto [Bertenthal93] identifican tres propiedades en la percepción humana al momento de caminar.

- Frecuencia de Relación de Fases (Frequency entrainment).- Es el proceso a través del cual dos sistemas interactuando en oscilación, los cuales tienen diferentes periodos cuando ellos funcionan independientemente pueden asumir un mismo periodo en un tiempo determinado. Varias relaciones de fase pueden ser posibles al momento de analizar la manera de caminar de las personas.

  Los componentes en la manera de caminar deben compartir una frecuencia en común; por ejemplo, no es posible caminar con movimientos en arbitrarias frecuencias.
- Fase del Cierre (Phase Loocking).- Es la relación de fase entre los componentes de la manera de caminar que permanecen aproximadamente constantes. El cierre varía en diferentes tipos de traslado como el de caminar, correr, etc.
- Plausibilidad Física (Physical Plausibility).- El movimiento debe ser físicamente un plausible movimiento humano.

Cuando los movimientos están en frecuencias de relación de fase, la fase del movimiento debe ser fijada (Fase del Cierre); por ejemplo, los patrones de movimiento en el tiempo pueden ser fijados cuando el movimiento del brazo izquierdo está en fase con la pierna derecha y opuesta en fase con la pierna izquierda.

Para entender la plausibilidad física, podemos considerar el movimiento de algún personaje de película de acción como Jackie Chan o Jet Li. Ellos realizan hazañas que no son creíbles sin utilizar cuerdas. Sin embargo, aún cuando las cuerdas no sean visibles a los televidentes, ellos saben que se encuentran ahí, pues los movimientos no podrían ser posibles.

Podemos concluir tres puntos importantes:

1. Identificar la oscilación de las señales que el sistema deriva de los movimientos cíclicos.
2. Determinar como la oscilación de las señales establece frecuencias de relación de fase, fase de cierre y plausibilidad física. Y
3. Determinar como la oscilación de las señales se puede trasladar dentro de características que pueden ser usadas para el reconocimiento.

Una característica importante en la manera de caminar, incluyendo el correr y el esprintar es su *simetría bilateral*.

4.2.2.1) Simetría Bilateral

Como ejemplo las piernas derecha e izquierda y los lados opuestos de los brazos se encuentran en una fase de cambio a la mitad de un periodo. Estos movimientos operan en espacio y tiempo, satisfaciendo las reglas de simetría espacial (intercambio de piernas) y simetría temporal (una fase de cierre en la mitad de un periodo).

En la figura 20 se observan ambas rotaciones de muslos y de rodillas para una persona caminando. Se asume que las piernas son osciladores emparejados a la mitad de un periodo o fase de cambio. Entonces, ambas piernas pueden ser modeladas por dos distintos osciladores emparejados, mientras que oscilen en la misma frecuencia (frequency-lock), pero con sus diferencias de fase relativamente fijadas.

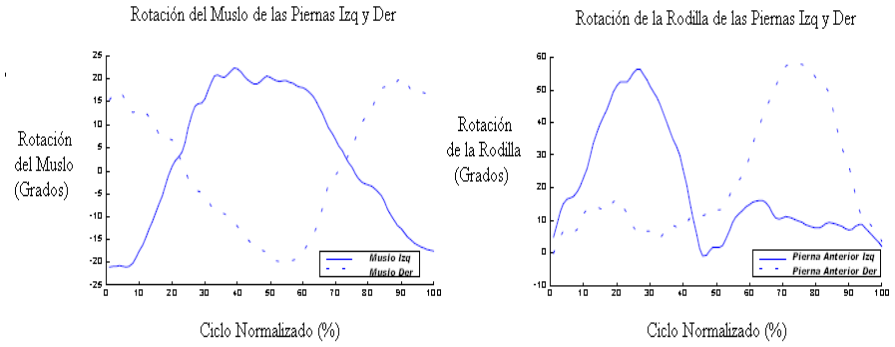


Figura 20.- (a) y (b) son la rotación de muslos y rodillas respectivamente a la mitad de un periodo de cambio

4.2.3) Substracción del Fondo

La substracción del fondo es un método para identificar objetos en movimiento desde una secuencia de imágenes [Kale04] en contra de un fondo. Aunque hay muchas variaciones sobre el tema, la idea básica es la siguiente:

1. Estimar las propiedades del píxel del fondo.
2. Substraer los valores actuales del píxel del fondo estimado, y
3. Asumir que si la diferencia del umbral dado del píxel excede, éste debe ser parte de un objeto en movimiento.

Normalmente se sigue el último paso formando conexiones, o manchas de píxeles en movimiento que correspondan a objetos en movimiento, se puede ver un ejemplo en la figura 21.

La selección del umbral para la imagen binaria es muy difícil, especialmente en el caso del bajo contraste de las imágenes [Wang02]. Esto es esencial en la eficiencia computacional y para la certeza en la extracción de características [Murray67].

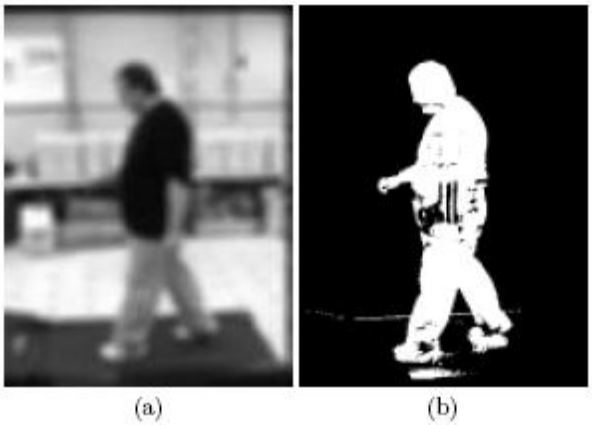


Figura 21.- Substracción de fondo tomada desde la base de datos de MoBo [Gross01]. (a) Imagen original (alterada para ocultar la identidad del individuo) y (b) Imagen segmentada

Los factores que afectan la substracción de fondos incluyen movimiento del fondo, movimiento de los objetos que son similares en apariencia al fondo, variaciones del fondo sobre largos periodos de tiempo y objetos en cercana proximidad emergiendo juntos. En general las variaciones sobre el tema de la substracción de fondos envuelven elegir pixeles para comparar modelos de fondos y para encontrar innovaciones sobre las adversidades que se vayan encontrando.

Como ningún algoritmo de detección de cambio es perfecto, *operadores morfológicos* pueden ser además usados para filtrar pixeles espurios [Wang02].

4.2.4) Siluetas

La substracción del fondo es un grupo de píxeles que se encuentran en movimiento dentro de una región de un objeto, dicha substracción la denominamos silueta, pero en la práctica puede que solamente nos pueda interesar el contorno de la silueta. *El reconocimiento de las personas mediante siluetas depende grandemente sobre como la silueta del cuerpo humano cambia en el tiempo.*

Podemos citar el siguiente ejemplo refiriéndonos al estudio del contorno de una silueta:

Después de que la silueta espacial ha sido extraída, sus límites pueden ser fácilmente obtenidos usando una frontera siguiendo un *algoritmo basado sobre la continuidad* [Wang02]. Entonces se puede calcular su figura centroide como se ve en la figura siguiente (Fig. 22).

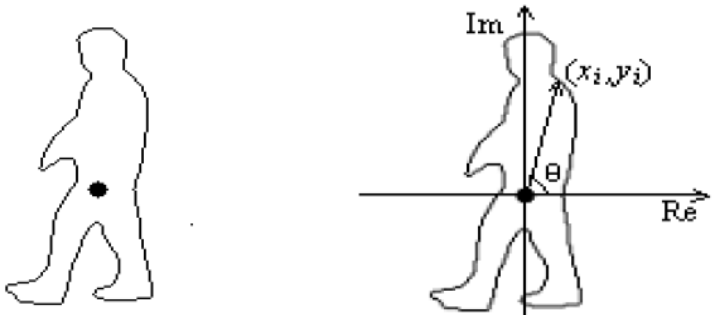


Figura 22.- Centroide obtenido mediante el contorno de una silueta

El método consiste en comparar un grupo de figuras de poses estáticas en los patrones de la manera de caminar y debe ser lo suficientemente robusto para la posición, escala y cambios en ligeras rotaciones. Un elegante camino matemático para realizar este estudio es por medio del *análisis de figuras de Procrusto.*

Dicho estudio puede ser una figura en espacio de 2-D descrita por un vector de *k* números complejos, $k=[z_1,z_2 ..., z_k]^a$, llamado "*configuración"*. Para dos figuras, z_1 y z_2, si sus configuraciones son iguales para una combinación de traslación, escala y rotación, se puede considerar que es la misma figura. No hay razón para esperar que las características extraídas sean invariantes a los ángulos de visión.

Información dinámica como las trayectorias oscilatorias de uniones o de los miembros pueden además ayudar al reconocimiento; por tanto, cuerpos humanos en 3-D podrían mejorar el reconocimiento de la persona caminando. Algunos ejemplos del análisis por la manera de caminar que usan siluetas se encuentran en Baumberg y Hogg [Baumberg95].

4.2.5) Flujo Óptico

Un campo de movimiento, es una proyección de movimiento en una escena dentro del plano de una imagen. El flujo óptico se refiere al movimiento o flujo de luminosidad del píxel en una secuencia de imagen. Aunque el campo de movimiento y el flujo

óptico no son lo mismo, muchas veces se usa el flujo óptico como una aproximación al campo de movimiento desde que muchos flujos son causados por observación de movimientos. Un ejemplo referente al flujo óptico lo podemos ver en la figura 23.

Los cambios de iluminación tales como reflexiones, sombras, movimiento de nubes, inter-reflexiones entre los movimientos de la figura y el fondo, y reflexiones de la figura en movimiento en superficies especulares en el fondo, contaminan la señal en movimiento [Little98].

Para disminuir el universo de elementos contaminantes, J. Little y J. Boyd [Little98] proponen un método para aislar los movimientos de la figura. Calculan el desplazamiento promedio de la persona a través de la secuencia de imágenes y utilizan el flujo en una sola "*ventana*". Para las pequeñas variaciones locales que quedan dentro de la ventana, eliminaron todos los puntos que no eran lo suficientemente grandes y conectados a las regiones.

Barron, Jepson y Fleet [Barron94] proveen una excelente vista general de varios algoritmos de flujo óptico que comparan su funcionamiento; ellos dividen los algoritmos dentro de cuatro categorías:

- Diferencial
- Relacionado a la región
- Basado en energía
- Basado en Fase

imagen 1

imagen 2

imagen 3

Figura 23.- Flujo Óptico de tres imágenes de una persona caminando

4.2.6) Métodos de estudio en la manera de caminar

Podemos discernir ahora que la biometría por la manera de caminar se sitúa prácticamente en 2 tipos de análisis: *basados en modelo y holísticos (o libres de modelo)*. Ambas metodologías usan el esquema de *extracción de rasgos*, *correspondencia de rasgos* y *un procesamiento de alto nivel*. Su mayor diferencia es con respecto a la correspondencia de rasgos entre dos tramas consecutivas.

4.2.6.1) Método basado en modelo

Los métodos que asumen un modelo a priori explícitamente modelan la estructura del cuerpo humano. La correspondencia de rasgos es automáticamente obtenida una vez que la relación entre las imágenes y los datos del modelo son establecidos. En orden para adecuar el modelo en la trama, parámetros estáticos tales como longitud de los miembros, estatura del cuerpo, anchura del cuerpo y parámetros dinámicos como velocidades angulares y la velocidad del caminante necesitan ser estimadas [Cattin02].

Ejemplos:

Cunado [Cunado99] propuso un método basado sobre el análisis de las características del movimiento de la pierna. Éstas fueron extraídas usando series de Fourier para describir el movimiento de la pierna y las correlacionó temporalmente para determinar el modelo dinámico de una secuencia de imágenes. El funcionamiento de esta técnica fue prometedor con tasas de reconocimiento de hasta el 90%; sin embargo, las muestras de la prueba fueron pequeñas [Green06].

Además, Cunado y otros [Bobick01] extrajeron muestras en el movimiento de las piernas a un articulado modelo de movimiento, el péndulo. La idea es algo similar a un temprano trabajo por Murray [Huang99] quien modeló el ángulo de rotación de la cadera como un simple péndulo, movimiento el cual fue aproximadamente descrito por un movimiento simple armónico.

4.2.6.2) Método holístico o libre de modelo

Es un método derivado de información estadística y es tratado como una secuencia de imágenes binarias, el cual establece la correspondencia entre tramas basadas sobre la predicción o estimación de características relacionadas a la posición, velocidad, forma, textura y color. [Kale04].

Ejemplos:

Los resultados iniciales son prometedores con tasas de reconocimiento tan altas como del 100% para pequeñas bases de datos de cientos de usuarios. Sin embargo, ninguna investigación ha sido hecha para establecer si estas altas tasas del reconocimiento se trasladarán a grandes bases de datos con miles de usuarios como en el reconocimiento de cara o aún con millones de usuarios como en el reconocimiento del iris [Daugman02].

Huang y otros [Cunado95] usaron el flujo óptico para obtener una secuencia de imágenes en movimiento para un ciclo del caminante. Análisis del Componente Principal es entonces aplicado a la silueta binaria de la imagen para obtener lo que son llamados *eigen gaits*. Además Little y Boyd [Bobick01] extrajeron características de frecuencia y fase de momentos de la imagen en movimiento, obtenidas del flujo óptico y usaron la relación de modelos para reconocer diferentes personas por su manera de caminar.

4.3) IDENTIFICACIÓN EN LA MANERA DEL CAMINAR

4.3.1) La manera de caminar como un modo de identificación

El campo del análisis en la manera del caminar se ha convertido en una herramienta para la medicina ortopédica y ha llegado a ser usada de manera importante para el diagnóstico y para propósitos de

rehabilitación. Estas investigaciones han mostrado que cada individuo tiene ciertos patrones que varían al momento de caminar y es por esto que pueden ser usados para su reconocimiento [Murray67].

El estudio del reconocimiento por la manera de caminar se puede encargar de reconocer tres propiedades:

- La identidad,
- Estilo de caminar o
- Alguna patología.

En nuestro trabajo nos enfocamos en el estudio del reconocimiento por la manera de caminar desde el punto de vista de identificación-autenticación biométrica.

4.3.2) Biometría por la manera de caminar

4.3.2.1) Objetivos en la implementación

- Debe ser barata en el sentido que el sistema final pueda ser de relevancia práctica y comercial,
- Debe ser eficiente computacionalmente para que la demora en la autenticación sea razonable y
- Debe ser lo suficientemente robusto para que los usuarios validos obtengan acceso y los impostores sean rechazados.

4.3.2.2) Cualidades Positivas

En respuesta a la creciente demanda en sistemas biométricos confiables y amigables, la manera de caminar tiene importantes propiedades que lo hacen un candidato interesante para ser un sistema biométrico competitivo.

- Las personas no necesitan interactuar con un sensor en un camino no natural. Sólo es necesario pasar por un lugar equipado con sensores especiales [Cattin02].
- En sensores de video o infrarrojos no es requerido ningún tipo de contacto físico con un sensor [Nixon99].
- Es amigable al usuario en el sentido de que ninguna otra interacción es necesaria más que el pasar por los sensores.
- Opera en una resolución de imágenes más baja que por ejemplo la biometría de detección de cara o iris [Green06].

- Desde que la manera de caminar es un biométrico conductual, entonces implícitamente se sabe que se tiene una muestra viva porque hay una persona en movimiento; por lo tanto no puede ser perdida o robada.
- Los usuarios no necesitan revelar información personal adicional más que la ya disponible.
- Los cambios de iluminación no son causa de serias preocupaciones.
- Puede ser capturado por cámaras conectadas a distancia.
- Es un biométrico que se percibe a distancia [Wang02].
- Existe menos probabilidad de ser ocultado que otros biométricos [Nixon99].

4.3.2.3) Factores que alteran la manera del caminar y el reconocimiento de los individuos

Diversos factores pueden modificar la manera natural del caminar o pueden complicar el proceso de autenticación ó identificación biométrica. Veamos la tabla 7.

FACTORES	**DESCRIPCIÓN**
Terreno	Lazlo y otros [Laszlo96] ilustran variaciones en la manera de caminar de un humano debido al terreno en gráficas por computadora.
Zapatos [Cattin02]	von Tscharner [Von03] mostró que la activación del músculo en los caminantes varía cuando las personas caminan descalzas a cuando usan zapatos.
Objetos	Llevando objetos que obstruyen las partes del cuerpo reducen la efectividad del biométrico; por ejemplo llevando objetos grandes en el brazo como una taza grande alteraría la manera dinámica en el caminar natural de un individuo. Llevando aún objetos más grandes como maletas, mochilas y bolsas sin duda se vería afectado el sistema de autenticación-identificación biométrico [Green06].
Ropa	La influencia en los cambios de ropa puede alterar al reconocimiento de un individuo. Además, el tipo de ropa, como suéteres gruesos de lana [Green06] o ropa holgada obstruyen las partes del cuerpo y esto reduce la efectividad del biométrico. Green y Guan [Green06] demostraron que aumenta la exactitud del reconocimiento mediante el uso de ropa ajustada.
Artefactos Culturales	Hace referencia al pavonearse con ciertas prendas, caminar con afectación, etc.
Idiosincrasia personal	Altera el caminar natural de un individuo.
Consciencia sobre la grabación	Cuando la persona está consciente de que está siendo captada por cámara(s), se puede generar cierta excitación o apatía, generando alteraciones en la manera del caminar.
El paso del tiempo	Altera el caminar natural de un individuo.
Desarrollo del músculo	Altera el caminar natural de un individuo.

Entrenamiento	Hace referencia cuando los atletas entrenan o cuando los militares marchan.
Lesiones	Murray y otros [Murray64, Murray67] describen variaciones en la manera de caminar de las personas debido a lesiones.
Fatiga	Altera el caminar natural de un individuo.
Embarazo [Nixon99]	Altera el caminar natural de una mujer.
Estado de Ebriedad [Nixon99]	Altera el caminar natural de un individuo.
Cabello [Green06]	Puede influir en el proceso de reconocimiento de un individuo.

Tabla 7.- Factores que alteran la manera del caminar y el reconocimiento de los individuos

4.3.2.4) Otros Factores

La adquisición de imágenes representando la manera de caminar del individuo pueden ser adquiridas fácilmente en áreas públicas con simple instrumentación, y no requieren la cooperación o aún el consentimiento de él o los individuos en observación.

Inclusive, esta biometría puede ser tan discreta que un sujeto puede que no se encuentre consiente sobre la vigilancia e identificación que pudiera ser llevada a cabo sobre él. Podría ser incluso éste, el método más discreto estudiado en la actualidad y con esto podemos entender ahora el grave problema que pudiese presentarse debido a la invasión a la privacidad.

Cada uno de estos factores debe ser analizado para tratar de encontrar una manera posible de eludir o solucionar cada una de las circunstancias arriba mencionadas. A continuación se analiza y plantea el caso del uso de *bolsas, mochilas* y *zapatos.*

Bolsas, Mochilas y Zapatos

Aunque uno puede asumir cierta cooperación de parte de los usuarios, uno no puede suponer que usen siempre la misma ropa y zapatos cuando usen un sistema biométrico. Por tanto, los sistemas biométricos deben tener cierta flexibilidad con respecto al cambio de ropa, incluyendo bolsas, mochilas y cambio de zapatos.

Tres posibilidades son declaradas:

1. Hacer al sistema insensible.
2. Formar casos especiales. Ó
3. Agregar equipo adicional para evitar tales situaciones.

La primera propuesta implica agregar instrucciones en los algoritmos de extracción de características para hacer insensible al sistema de los usuarios que portan diferentes mudas de ropa. Ejemplos incluyen algoritmos de segmentación de imágenes adaptivas que son insensibles a cambios en el color de la ropa o a condiciones de luz.

La segunda propuesta es un enfoque muy pragmático. Podría prepararse al sistema con por ejemplo diferentes pares de zapatos y entonces hacer al reconocimiento más tolerante. Aunque esta propuesta es factible, debe ser evitada, pues incrementaría el número de secuencias de aprendizaje requeridas y provocaría el desagrado de los usuarios.

La tercera y última propuesta sería, usar equipo adicional para mejorar la calidad del reconocimiento. Un posible escenario sería sombrear la sensibilidad con segmentación de imágenes usando iluminación de fondo (backlight). El aumentado contraste persona/fondo casi completamente eliminaría las dificultades de la segmentación. Otro posible escenario es proveer una banda transportadora, similar a los detectores de metal en los aeropuertos, donde los usuarios pueden poner sus mochilas o bolsas antes de pasar al área de medición.

Cattin P. [Cattin02] realizó un estudio basándose en la propuesta pragmática; donde por medio de un sensor de fuerza muestra la influencia en el resultado de las muestras obtenidas por medio del uso de diferentes pares de zapatos en un mismo usuario (Ver figura 24).

El resultado obtenido fue que cuando el usuario usó el mismo par de zapatos, las muestras extraídas eran muy similares entre sí, mientras que cuando se utilizó un par diferente de zapatos, las muestras extraídas tenían variaciones significantes.

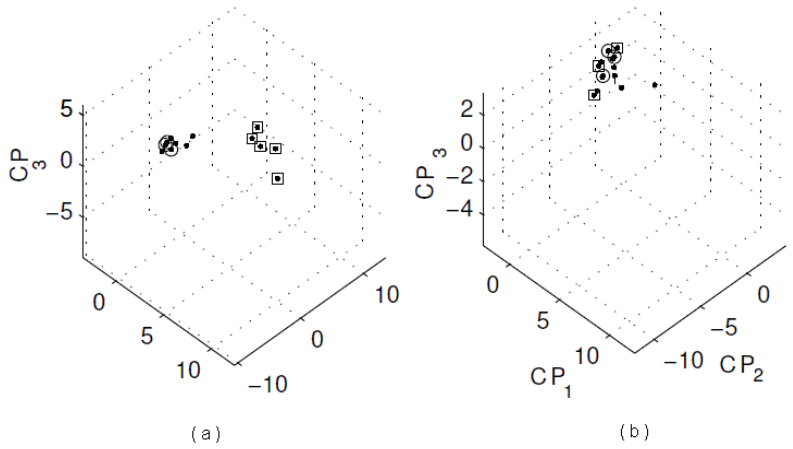


Figura 24.- Análisis del Componente Principal.- (a) Los 5 rasgos característicos marcados por "." y los 3 rasgos característicos marcados por "⊙" fueron tomados con el mismo par de zapatos (zapatos de suela baja). Claramente se puede ver que forman un compacto grupo de rasgos característicos similares, mientras que los otros 5 rasgos característicos marcados con "⊡" forman otro grupo diferente pues fueron tomados con un diferente par de zapatos (sandalias). (b) Diferentes pares de zapatos, desde zapatillas hasta botas de montaña fueron agregados en la fase de capacitación al sistema y al momento de extraer los rasgos característicos se obtuvo un grupo similar de rasgos característicos

Como lo demostró Cattin, la elección de un par de zapatos influye sobre la adquisición de muestras, sin embargo clarificó que el problema puede ser resuelto incorporando varios pares de zapatos durante la fase del entrenamiento en el sistema. Entonces el sistema fue posible de aprender diferentes pares de zapatos al momento de la extracción de características y se mejoró la función del reconocimiento.

Mochilas y Bolsas

Cattin aplicó este mismo experimento en personas usando bolsas y maletas y explicó que el sistema puede ser entrenado para que el usuario se enfrente al sistema con o sin una maleta o una bolsa. Sin embargo, la propuesta de incluir adicional entrenamiento en los sistemas para mejorar el reconocimiento no siempre produce los resultados esperados. Figura 25.

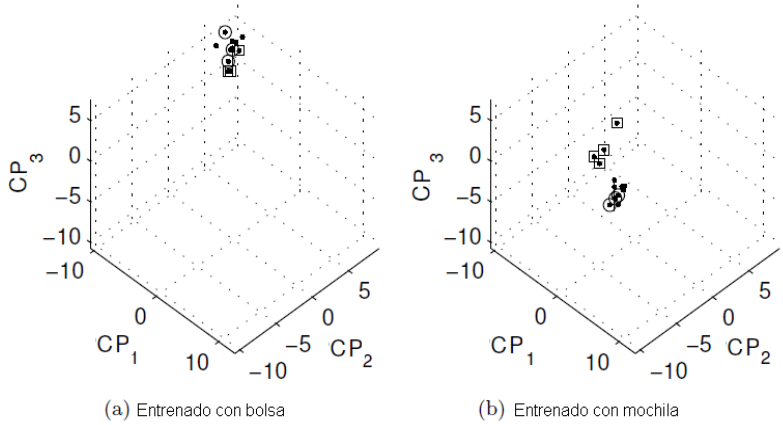


Figura 25.- Análisis del Componente Principal.- (a) Bolsa sobre el hombro izquierdo. (b) Mochila. Aunque dos adicionales entrenamientos por la manera de caminar con una mochila fueron agregados en el escenario de entrenamiento, todavía se encuentran dos grupos distinguibles de rasgos característicos

4.3.2.5) Métodos de aceptación o rechazo en la autenticación - identificación

Estrategias como *percerptrón multicapas* (redes neuronales artificiales) y *árboles de decisión* son utilizados para decidir la identidad de una persona. Otra técnica más simple es formar un *vector característico*, que contenga información de todos los sensores a analizar. Sin embargo está es computacionalmente cara y solamente es exitosa cuando se tienen todas las características estadísticamente comparables y un gran potencial discriminatorio.

Otra técnica es el sensor multi-modelo, que es una típica arquitectura en paralelo de un sistema fusión (Figura 26). El usuario cada vez que reclama su identidad proporciona un nuevo modelo. Entonces, cada una de las diferentes modalidades N tiene su propio experto local que compara el nuevo modelo al modelo asociado a la identidad reclamada. Todos ellos producen una relación-de-resultados (*resultado* $_i$) que expresa la opinión de su respectivo experto local, el cual se basa sobre la información disponible. Entonces el experto global combina las opiniones de los diferentes expertos locales y realiza una decisión final aceptando o rechazando a ese particular usuario.

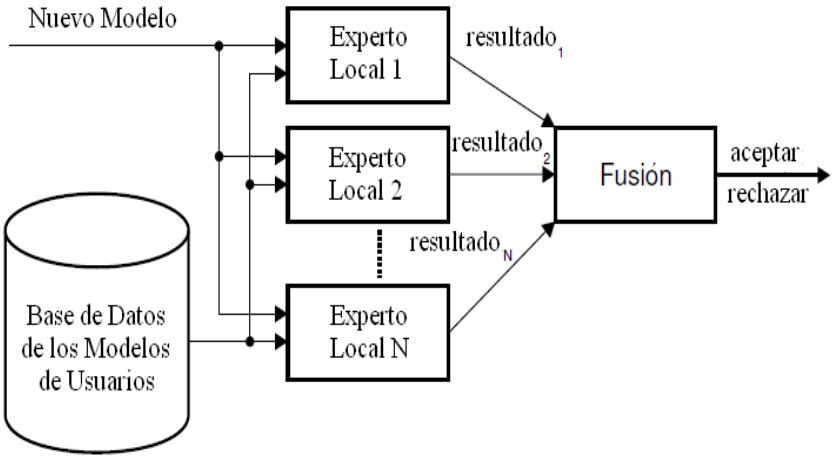


Figura 26.- Principio de un esquema de fusión en paralelo. Multi-modelo

La verificación de la identidad en un sistema multi-modelo es una prometedora investigación. Combina la ventaja de las diferentes modalidades y tiene el potencial para compensar las debilidades de otras. En particular la fortaleza del sistema biométrico puede ser drásticamente mejorada.

Hay muchas reglas de combinación de decisión posibles, como *max, min, sum, rank-sum*, etcétera. [Liu04]

4.3.2.6) Tipología conductual

La biometría por la manera de caminar es parte del estudio de la tipología conductual[1].

Debido a las inevitables variaciones en los rasgos conductuales, muchos sistemas usan un mecanismo para actualizar el modelo de referencia en orden para compensar los cambios sobre el tiempo. Generalmente la biometría conductual trabaja mejor con el uso regular.

4.3.2.7) Complejidad Computacional

La complejidad biométrica computacional es crucial, pues limita al número de usuarios que pueden ser diferenciados y puede informalmente ser aproximada con la pregunta:

[1] Ver el apartado: 3.3 Tipología de la tecnología biométrica.

- ¿Cómo cuántas distinguibles maneras de caminar existen en el proceso?

Sin embargo esta fácil pregunta, según [Phillips00], todavía no es capaz de establecer un límite en muchas tecnologías, incluyendo a la manera de caminar. Aunque si podemos decir que es de ingresos intensivos de datos y computacionalmente cara [Jain04].

4.3.3) Ambientes Exteriores y Ambientes Interiores

Una muestra biométrica recolectada en un ambiente externo no controlado varia significativamente de la de un ambiente interno controlado. Las variaciones de las muestras debido a condiciones en ambientes externos degradan el funcionamiento del sistema biométrico que por lo regular se ejecutarían bien en un ambiente interno.

Por ejemplo, la biometría por la manera de caminar es importante para aplicaciones de vigilancia pues es importante ser capaz de establecer identidades a distancia. Sin embargo no es lo suficientemente robusta para tener un alto reconocimiento de confianza en ambientes externos, especialmente respecto al tiempo.

Una de las ventajas en ambientes internos es que muchas veces se asume que entre el campo de visión de la cámara estacionaria existe solamente una persona en el momento de la captura de imágenes y esto simplifica grandemente el proceso [Naresh03].

4.3.4) Sensores

Algunos sensores para medir la manera de caminar pueden ser:

- Sensores de Fuerza que miden la fuerza de la reacción del terreno perpendicular al piso.
- Sensores de Video que capturan una vista de un sujeto que está pasando.
- Sensores de Luz Infrarroja (IR) para además captar imágenes en la noche.

4.3.4.1) Muestra y Modelo

El HumanID Gait Challenge Problem [Phillips02], reportó que para actuales algoritmos de reconocimiento por la manera de caminar, se están comparando modelos por 6 meses de diferencia y la tasa de verificación no es mejor que el 24% en 1% de falsas alarmas [Liu04].

La adquisición de muestras para el reconocimiento sobre periodos largos de tiempo; meses, incluso semanas, y la variedad de condiciones al adquirir las imágenes, como la extracción de imágenes con más de un aparato, afectan drásticamente las tasas del reconocimiento; aunque son beneficiadas incrementando la medida de la muestra ya que ayudan a dimensionar mejor el cuerpo humano dando origen a una mayor precisión [Green06]. Pero si la muestra es demasiado grande, el espacio asignado para las muestras puede ser sobresaturado y si las bases de datos continúan creciendo en medida, sería imaginable que identificar a una persona solamente por su manera de caminar podría ser difícil. Sin embargo, la manera de caminar podría servir como un filtro que nos permitiera reducir un considerable grupo más pequeño de potenciales candidatos [Kale04].

A diferencia de otros biométricos como el de impresión de huella; en la biometría por la manera de caminar no se puede saber que tan extensas deban de ser las muestras, como para satisfacer la unicidad del biométrico.

4.3.4.2) Cámaras

4.3.4.2.1) Posicionamiento de la Cámara

La adquisición de imágenes en ángulos inesperados puede invalidar el rastreo y reconocimiento del caminante. En la mayoría de los métodos para el reconocimiento, la manera de caminar de la persona es fácilmente reconocible cuando los rasgos característicos son extraídos desde una visión lateral a la cámara. Por consiguiente, los algoritmos de reconocimiento trabajan mejor cuando son presentados con imágenes donde la persona camina en paralelo a la cámara (por ejemplo, una imagen plana). Sin embargo no es realista esperar que esta suposición sea válida en todos los escenarios de la vida real. Por tanto es importante desarrollar métodos según los cuales la vista de lado pueda ser generada desde alguna otra arbitraria vista en otro distinto ángulo. Amit Kale y otros [Kale03] demostraron que si la

persona está lo suficientemente lejos de la cámara, es posible constituir una vista de lado (referida como una *vista canónica*) desde alguna otra arbitraria vista, usando una simple cámara.

Además con un espejo posicionado en dirección a la cámara y al sujeto que se encuentra caminando se pueden obtener vistas complementarias del caminante. Tal es el caso de [Murray67] que posicionó un espejo por encima de la persona caminando para que su cámara llegase a obtener una vista superior del caminante y así captar imágenes del balanceo del hombro de la persona, las cuales son de gran valor para la verificación de la identidad.

Como podemos intuir la posición del sujeto hacia la cámara es importante para la extracción de los rasgos característicos, pero además hay factores que contribuyen a la distorsión en la extracción de los rasgos; como la *inclinación de los ángulos del muslo* que distorsionan en movimientos frontoparalelos los movimientos cercanos y lejanos de un mismo individuo [Spencer02].

Hay dos efectos que pueden acontecer a la vista debido al posicionamiento de las cámaras. Uno es simplemente el escorzo o la lejanía que ocurre cuando la persona camina a lo lejos o hacia la cámara. El segundo es el cambio en la aparente longitud de la zancada. La solución más general a este problema podría envolver un *modelo 3-D* de la persona; ya sea creando una vista canónica [Kale03] o por medio de un ambiente multicámara.

Podemos apreciar que entre más cerca se encuentre la cámara al objeto en movimiento se tendría una mejor vista de la imagen, pero reduciría el número de secuencias a grabar [Little98]. Para métodos que utilicen como base de estudio el ciclo de un caminante, hay que tener en cuenta que por lo menos la(s) cámara(s) tiene(n) que captar dos pasos para incluir un ciclo completo.

Debido a lo mencionado, un punto clave en el reconocimiento en la manera del caminar es la distancia entre la cámara y la persona en movimiento.

4.3.4.3) Sensores de Fuerza

4.3.4.3.1) Rasgos Característicos

Si se pretenden implementar sensores de fuerza de reacción se debe tener en consideración la manera en cómo deben ser colocados.

Imaginemos que los sensores se colocan de manera tal, que la persona tenga que colocar sus pies en un lugar específico (Figura 27 a); las personas altas con longitudes de zancadas largas tendrían que acortar sus pasos significativamente y les impediría caminar en su manera natural y acostumbrada. Esto resultaría en una extracción de rasgos inconsistentes e impredecibles.

Lo mejor es tener un escenario que haga sentir al usuario lo más natural posible sin el conocimiento específico del lugar donde se encuentran colocados los sensores, de tal manera que el usuario no intentase de manera premeditada pasar por un lugar específico provocando un caminar distinto al natural (Figura 27 b).

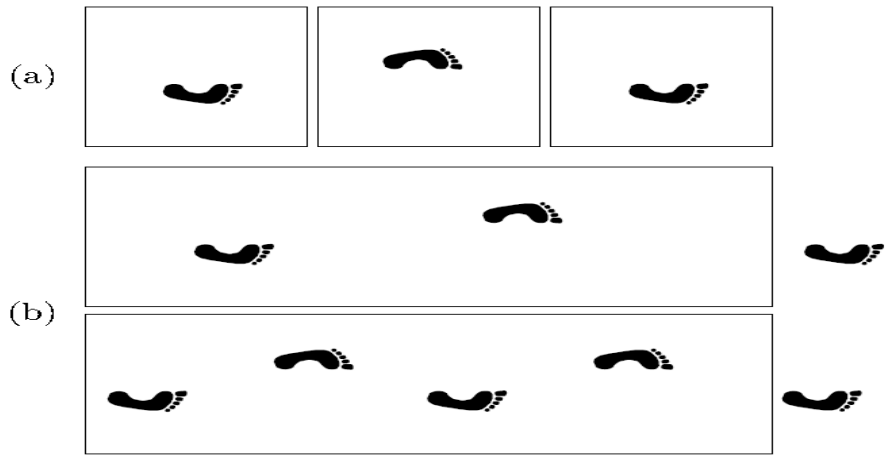


Figura 27.- a) Personas altas y pequeñas que adecuan sus pies en cada uno de los platos al caminar. b) Personas altas y pequeñas que son libres de colocar sus pies al caminar sin preocuparse de los platos

4.3.5) Características a medir en el reconocimiento por la manera de caminar

En un principio, la mayoría de los algoritmos elegían las manos y piernas como los rasgos más importantes a analizar en el momento

de reconocer personas, pero las manos muchas veces son restringidas en su movimiento por objetos que lleva la persona. También en métodos de substracción del fondo muchas veces se encuentran secuencias excesivamente ruidosas en la región del torso, entonces la dinámica de la pierna es la que por lo regular lleva la mayor parte de la información acerca de la manera del caminar.

Estudios llevados a cabo en varias partes del cuerpo sugieren que la región de la pierna puede presentar un más consistente patrón comparado a otras partes del cuerpo tales como los brazos. El funcionamiento en el caso donde la información de la estatura es fusionada con la dinámica de la pierna es aún mejor, debido a que la estatura puede ser usada como un útil discriminador de objetos [Kale03].

Cuando se cuenta con vistas frontoparalelas y de lado frontal, se pueden combinar para obtener una decisión final para la identidad de la persona. Un camino para combinar múltiples vistas es mediante el uso de modelos 3-D [Naresh03].

Aún en una vista frontal donde el aparente balanceo de la pierna/brazo es el más deficiente, se pueden encontrar varias entradas que pueden ser usadas para el reconocimiento del humano; como la postura de la cabeza, el contoneo de la cadera, movimientos de oscilación de la parte superior del cuerpo, etc.

En la tabla 8 menciono algunos de los rasgos más importantes que se pueden analizar al momento de implementar un algoritmo en el reconocimiento por la manera de caminar.

Características	***Descripción***
El periodo	*Estudio del ciclo en la manera de caminar*
Cuerpo humano	*Dimensiones del cuerpo humano, como la longitud de los miembros o la estatura*
Dimensiones Esqueléticas	*Las medidas del esqueleto humano*
Postura	*La postura del cuerpo al momento del caminar*
El brazo	*Amplitud del balanceo* *Asimetría en el balanceo*
Hombro	*Balanceo*
Manos	*Posición y medida de las manos*
Manos-piernas	*Balanceo*
Cadera-cuerpo superior	*Contoneo*
Cadera-rodilla	*Asimetría y ángulos*

Muslo y rodilla	*Rotación del muslo y la rodilla [Yam01]*
Brazo-pierna	*Balanceo*
La zancada	*Amplitud*
Fuerza de reacción del terreno cuando la persona se encuentra caminando	*Fuerza anterior/posterior* *Fuerza vertical* *Fuerza lateral/media*

Tabla 8.- Rasgos característicos importantes a medir en el reconocimiento de los individuos

Citemos un pequeño análisis de la fuerza de reacción del terreno:

Los componentes de fuerza anterior/posterior Fx y vertical Fy son valores grandes, mientras que el componente de fuerza restante lateral/media Fz es el más pequeño en valor y sirve para propósitos de balance principalmente. La fuerza anterior/posterior, por ejemplo, es la fuerza de aceleración y desaceleración en la dirección del caminante y como tal depende sobre la estructura ósea y sobre los músculos de la persona.

Como demostración ilustro en la Figura 28 vectores característicos por medio de *un espectro de densidad de potencia* en la fuerza anterior/posterior de tres diferentes personas con dos muestras cada uno. Es claramente visible, que los vectores característicos de la misma persona (a+d, b+e, c+f) muestran grandes similitudes, mientras que el vector característico de entre las tres personas difiere substancialmente.

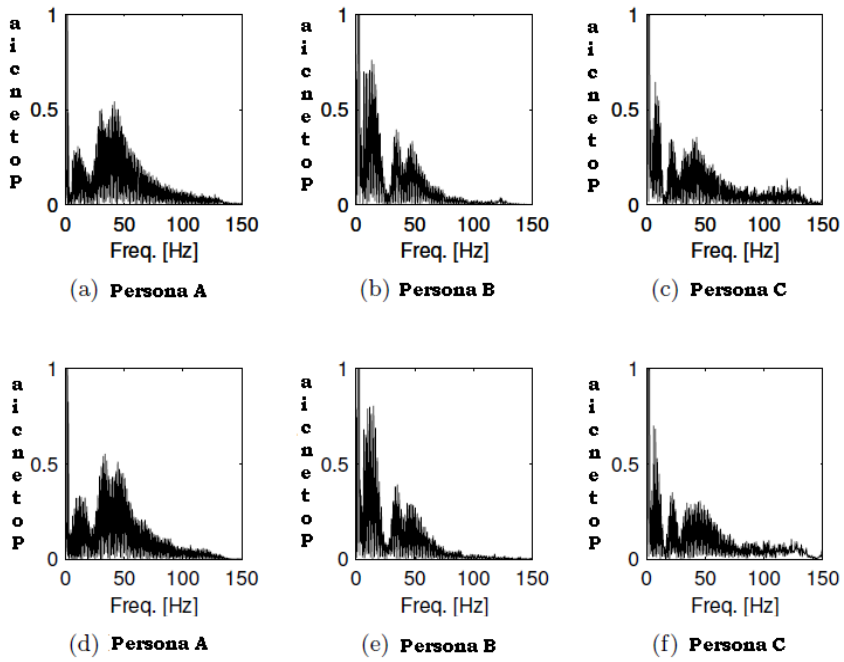


Figura 28.- Vectores característicos por la Fuerza de Reacción del Terreno de la fuerza anterior/posterior Fx para tres personas con dos vectores muestra cada uno

4.3.5.1) Cuasi-Reconocimiento por la manera de caminar

Hago la distinción entre el reconocimiento por la manera de caminar y lo que podemos definir como el cuasi reconocimiento por la manera de caminar; esta última como la propiedad basada sobre las características adquiridas mientras un sujeto está caminando, pero las características no son inherentemente parte de la manera de caminar.

Por ejemplo, las dimensiones esqueléticas las podemos medir durante el caminar de un individuo; sin embargo, éstas pueden ser medidas en otros caminos y por tanto, no son una propiedad exclusiva de la manera del caminar.

Una ventaja en el enfoque del cuasi reconocimiento por la manera de caminar es que son menos sensibles a las variaciones.

Ejemplos:

Bobick y Johnson [Bobick01] miden un grupo de cuatro parámetros que describen una estática pose extraída desde una secuencia por la manera de caminar. Estos parámetros son estatura, longitud del torso, longitud de la pierna y longitud de la zancada[2], todos los cuales pueden ser estimados desde una simple imagen como lo vemos en la Figura 29. Bobick y Johnson usan estos parámetros como características de vectores para el reconocimiento.

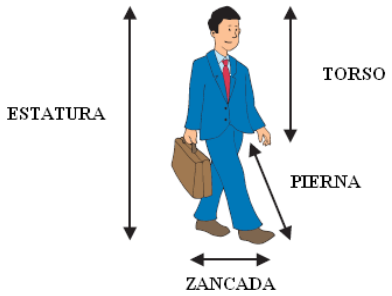


Figura 29.- Características estáticas medidas por Bobick y Johnson: Estatura, longitud del torso, longitud de la pierna y longitud de la zancada

[2] Comúnmente el término *longitud de paso* es mal empleado como un sinónimo al de *longitud de zancada*. La longitud del paso es la distancia desde un punto de contacto dado en el piso, por ejemplo, el talón izquierdo, al mismo punto de contacto del piso del otro pie, por ejemplo, el talón derecho. La longitud de la zancada por el otro lado, incluye la longitud de un paso izquierdo y de un paso derecho y entonces es la distancia cubierta de un ciclo en la manera del caminar. En esta cita no modificaré lo declarado por el autor para respetar la integridad de su artículo, pero hago hincapié en el verdadero significado del término cuando haga referencia a éste en mi investigación.

Otro ejemplo puede ser citado con Ben-Abdelkader y otros [Ben-Abdelkader02] quienes extrajeron la estatura de la persona, la amplitud de las oscilaciones de la estatura durante la manera de caminar, la cadencia[3] y la longitud de la zancada (ver Figura 30). Ellos entonces usan estos valores en un vector característico para el reconocimiento.

Aunque las características incluyen la cadencia, el método no usa información de tiempo en la manera de caminar, así que lo clasificaron como cuasi reconocimiento por la manera de caminar. Lograron una tasa de reconocimiento del 49% adquirida sobre dos días. Además miraron submuestras para determinar el funcionamiento deteriorado de la medida de la muestra. Los resultados son trazados en la figura 32.

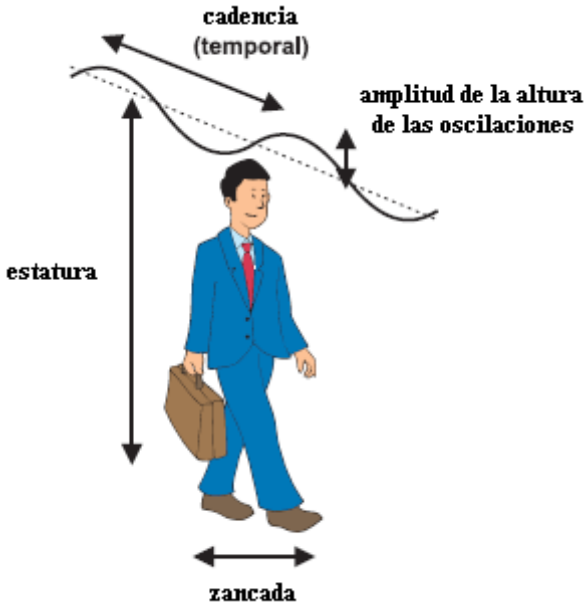


Figura 30.- Estatura, cadencia, amplitud de la altura de las oscilaciones y zancada [Ben-Abdelkader02]

Es percibido que estos métodos requieren cierta calibración de cámara y conocimiento de la distancia entre la cámara y la persona.

Finalmente, la velocidad es otro parámetro que podemos tomar como cuasi-reconocimiento por la manera de caminar el cual puede ser combinado con la longitud de la zancada y la cadencia para expresar la distancia cubierta en dirección de progresión por unidad de tiempo [Murray67].

[3] La cadencia se refiere al número de pasos por tiempo.

4.3.5.2) Velocidad en el caminar

Hay un considerable cambio en la dinámica del cuerpo humano y en la longitud de su zancada cuando una persona camina despacio y cuando una persona camina rápido. Observe la figura 31 en la cual se muestra a una persona en estos dos escenarios.

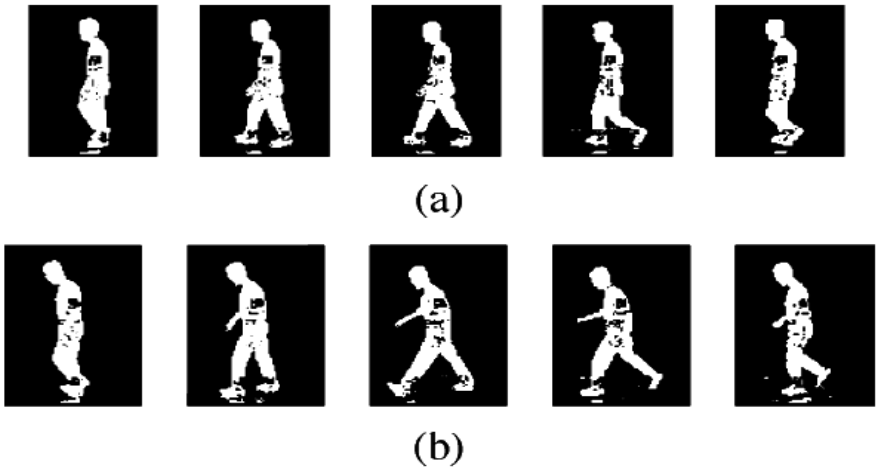


Figura 31.- Imágenes de muestra de una persona caminando. (a) Caminar despacio (b) Caminar rápido. Como se puede ver la postura como el balanceo de la mano son completamente diferentes cuando se camina con una diferente velocidad

4.3.6) ¿Qué características serían usadas?

Para obtener una tasa alta de reconocimiento, características discriminatorias deben ser extraídas de los datos disponibles. Desde un punto de vista ingenuo, parecería obvio tratar de reconocer a personas por la longitud de su zancada, cadencia, peso, estatura, etc. Sin embargo, estas características podrían ser no ideales para un sistema biométrico. De hecho, son altamente inseguras debido a su naturaleza estática, que permite a un impostor fácilmente imitarlas; por ejemplo, un impostor podría ajustar fácilmente su peso, longitud de zancada y/o cadencia para relacionarlas a un usuario legítimo y así tratar de obtener acceso a un área restringida.

En cambio, las propiedades dinámicas en la manera de caminar son mucho más difíciles de imitar, desde que ellas dependen sobre propiedades fisiológicas del cuerpo del usuario tal como la estructura ósea.

4.3.7) Extracción de Características

Diferentes maneras de extraer características en la manera de caminar han sido propuestas, sin embargo podemos dividirlas en dos grupos:

1. Sistemas que *necesitan* ubicar un paso o un ciclo completo para extraer los rasgos característicos. Donde cada una de las secuencias en la manera de caminar es representada por un simple punto. La principal ventaja se encuentra en lo relativamente fácil de su clasificación. Sin embargo podría ser difícil ubicar el ciclo y

2. Sistemas que *no necesitan* ubicar el ciclo entre los datos adquiridos, pero sus características varían sobre el tiempo. Estos sistemas generalmente usan HMM (Modelo Oculto de Markov - Hidden Markov Model) para reconocer y diferenciar personas desde sus trayectorias. La principal ventaja de este método se encuentra en la posibilidad de reconocer personas sin un completo ciclo, pero la clasificación final es ligeramente más difícil.

Refiriéndome al primer caso un punto de vista práctico en las mediciones del caminante, un reconocimiento robusto debería contemplar varios ciclos por la manera de caminar antes de tomar una decisión [Kale04].

Ninguna de las dos investigaciones es en sí mejor que la otra, meramente es un camino para clasificar los métodos.

4.3.8) Estado del Arte

Podemos entender que se pueden adquirir una gran variedad de tipos de muestras para el propósito de reconocimiento. Subsecuentemente podemos entender la dificultad de comparación entre diferentes sistemas biométricos a no ser por los resultados de un objetivo en particular [Little98].

Para dirigir esta cuestión en sí, la figura siguiente traza la tasa de reconocimiento de diferentes sistemas biométricos contra la medida de la muestra tomada. Entiéndase aquí que la siguiente figura solamente tiene el objetivo de mostrar *una figura aproximada del estado del arte en el reconocimiento de la*

manera de caminar y NO de mostrar las cuestiones que se encuentran en el momento del muestreo.

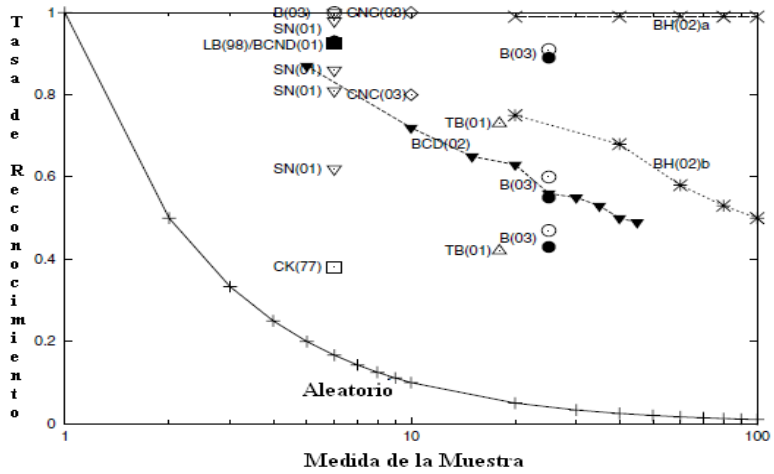


Figura 32.- Comparación del funcionamiento de los sistemas biométricos por el reconocimiento de la manera de caminar, mostrando la tasa de reconocimiento contra la medida de la muestra. La curva etiquetada ***Aleatorio*** *indica la tasa esperada de reconocimiento para las personas que fueron acertadas de manera aleatoria.* ***CK(77)*** *se refiere a Cutting y Kozlowski [Cutting77],* ***BH(02)a*** *y* ***BH(02)b*** *se refieren a Bhanu y Han [Bhanu02] 5mm y 40mm de resolución respectivamente,* ***LB98*** *se refiere a Little y Boyd [Little98],* ***BCND(01)*** *se refiere a Ben-Abdelkader y otros [Ben-Abdelkader01],* ***SN(01)*** *se refiere a Shutler y Nixon [Shutler01],* ***TB(01)*** *se refiere a Tanawongsuwan y Bobick [Tanawongsuwan01],* ***CNC(03)*** *se refiere a Cunado y otros [Cunado03],* ***B(03)*** *se refiere a Boyd [Boyd03] y* ***BCD(02)*** *se refiere a Ben-Abdelkader y otros [Ben-Abdelkader02]*

4.3.9) Estudios Complementarios

Los métodos que a continuación menciono pueden hacer o no, el reconocimiento por la manera de caminar, o no en su totalidad. Su justificación de estar escritos en esta investigación es complementar la visión general en el análisis de la biometría por la manera de caminar:

Polana y Nelson [Poana98] examinan oscilaciones en la magnitud del flujo óptico en una secuencia conteniendo movimientos periódicos. Ellos calculan una ordinaria imagen de magnitud de flujo de una resolución (cuatro por cuatro) de seis puntos en el periodo del movimiento. De esto ellos forman un vector de 96 elementos que es usado para reconocer un gran rango de movimientos periódicos, pero no para la manera de caminar de los individuos.

Liu y Picard [Liu98] examinan oscilaciones en la intensidad del píxel para una secuencia por la manera de caminar usando

Transformadas de Fourier rápidas (FFT por sus siglas en inglés Fast Fourier Transforms). Sus análisis identifican la amplitud de la frecuencia fundamental de la manera de caminar. Ellos no usaron la fase en sus análisis, no hicieron reconocimiento.

Baumberg y Hogg [Baumberg93] describen un método que extrae las siluetas de una figura caminando. Ellos extienden el concepto tratando cambios en la figura con un modelo en vibración [Baumberg95]. Ellos no reportan pruebas de sus modelos para el reconocimiento.

Desde una secuencia de imágenes, Davis y Bobick calculan los movimientos de imágenes de energía (MEI por sus siglas en inglés Motion Enery Images) y el historial del movimiento de las imágenes (MHI por sus siglas en inglés Motion-History Images) que indican donde los movimientos están ocurriendo y que tan recientemente el movimiento a ocurrido. Ellos describen la figura de las regiones en movimiento con un grupo de momentos Hu, los cuales ellos en turno usan para reconocer los patrones de movimiento, tales como varios ejercicios aeróbicos.

Varios métodos existen para relacionar un modelo cinemático de un humano a una secuencia de imágenes de video, por ejemplo, estimar la pose de un sujeto. En general, estos métodos no son específicos para la manera de caminar, no son ellos intencionados para hacer el reconocimiento. Ellos pueden ser vistos como métodos para captura en movimiento "sin rotuladores" (Marker-less. Para una mejor comprensión se puede consultar [German04]). Ejemplos de estos métodos incluyen los trabajos de Hunter y otros [Hunter97], Rowley y Rehg [Rowler97], Wachter y Nagel [Wachter97], Wren y otros [Wren97], Bregler y Malik [Bregler98] y Morris y Rehg [Bissiacco01]. Un problema con algunos sistemas basados en modelos es que los hacen o muy lentos o muy caros para el uso en un sistema biométrico.

Bissacco y otros [Bissiacco01] extienden los resultados de la adquisición de poses cinemáticas para el reconocimiento. Ellos usan el método Bregler [Bregler97] para extraer la unión de trayectorias de ángulos desde una secuencia en movimiento. Ellos entonces calculan un modelo promedio en movimiento auto-regresivo (ARMA por sus cifras en inglés Auto-Regressive Moving-Average) del movimiento de las articulaciones los cuales ellos en turno usan como un vector característico para el

reconocimiento. Su sistema puede reconocer diferentes tipos de maneras de andar tales como correr, caminar o subir escaleras. Aunque ellos no lo probaron en la biometría del reconocimiento por la manera de caminar, esto queda como una posibilidad.

Davis y otros [Davis97] y [Davis99] propusieron un método para reconocer las acciones y los gestos humanos usando dos diferentes variantes de modelos temporales:

1. Una imagen de energía en movimiento binaria (MEI Motion-Energy Image) la cual representa donde el movimiento ha ocurrido en una secuencia de imágenes y
2. Una imagen de historial en movimiento (MHI Motion-History Image) la cual es una imagen escalar valorizada donde la intensidad es una función de casi un actual movimiento.

CONCLUSIONES

A lo largo de mi investigación me he preocupado en el detalle para tratar de abarcar el mayor número de situaciones que se puedan presentar al momento de estudiar a la manera de caminar de las personas como un sistema de autenticación biométrico.

A continuación completo mi investigación concluyendo que *la manera de caminar de las personas puede ser usada como un sistema de autenticación biométrico, siempre y cuando se tenga en cuenta un estudio amplio y bien analizado, adecuado a las necesidades de cada situación en particular.*

Empezaré comentando que la seguridad no sólo en sistemas de autenticación biométrica sino en cualquiera no es hacer a un sistema de cómputo totalmente seguro, pues no es posible hacerlo ni físicamente ni técnicamente. El objetivo por tanto, es hacer el costo de un ataque lo suficientemente alto como para reducir el riesgo de los activos a niveles aceptables. Ya que la seguridad generalmente eleva los costos y la complejidad de un sistema debido a sus innumerables vulnerabilidades; antes de implementar seguridad en un sistema, es necesario identificar sus amenazas, y una vez identificadas, se sabrá en contra de que se deberá proteger y que se va a proteger.

Por esto, nuestro trabajo de investigación no puede definir todas las vulnerabilidades y amenazas que se encontrarán cuando sea implementado un sistema de autenticación biométrica por la manera de caminar; así mismo no es posible definir un modelo a seguir para implantar esta tecnología debido a que cada situación siempre será diferente a cada escenario en particular. Pero lo que sí hemos podido realizar, es un estudio detallado sobre la biometría por la manera de caminar de las personas para que el lector pueda por sí mismo analizar e identificar de una manera vasta e inteligible la protección de sus activos y recursos para así tomar mejores decisiones.

Se concluye que, los cuatro métodos de autenticación están conformados por cuatro niveles de seguridad o escenarios:

Nivel de Seguridad	Método de Autenticación		Usos	Seguridad	Coste	Uso Multifactor
Nivel 1	Alguna cosa que se conoce		Niveles de sensibilidad bajos	Baja	Bajo	Dependiendo de los mecanismos de seguridad justificados con la valoración de las amenazas, riesgos y contramedi-das, se pueden llegar a ajustar niveles de seguridad mayores y más adecuados a las necesidades
Nivel 2	Alguna cosa que se tiene		Nunca debe ser usado para información sensible, confidencial o clasificada	Media	Alto	
Nivel 3	Algu-na cosa que se es	Proceso Manual	Niveles de sensibilidad bajos, muchos de ellos para brindar un servicio al cliente	Baja	Bajo	
		Proceso Automa-tizado	**PARA AUTENTICAR A INDIVIDUOS**	Depende el biométrico	Medio/ Alto	
Nivel 4	Algo basado en la ubicación		Sector militar y aviación	Muy alta	Alto	

Pero, ¿Cuál de los cuatro métodos de autenticación es el más adecuado? La respuesta depende de la valoración que se haya hecho de las amenazas, riesgos y contramedidas para justificar el nivel de seguridad deseado para implementar el o los mecanismos de seguridad adecuados. Inclusive si se requieren niveles de seguridad más altos se pueden implementar esquemas multi-factor y/o híbridos.

Pero lo que sí se puede concluir, es que el método más conveniente para la autenticación de individuos es la biometría; ya que los demás métodos de autenticación se basan en identificar un ente no propio del individuo como una tarjeta, una contraseña o un SPG y no a un individuo como tal.

Para que una tecnología llegue a ser considerada biométrica se debe contar indispensablemente con los siguientes cuatro rasgos característicos:

- **Universalidad.**– Cada una de las personas debe tener las características.
- **Distinción de Rasgos.-** Entre dos o más personas, las características deben ser lo suficientemente diferentes para poder distinguirse.

- **Permanencia.-** Las características deben ser lo suficientemente invariantes sobre un periodo de tiempo.
- **Recolectadas.-** Las características puedan ser medidas cuantitativamente.

Se concluye que *la manera de caminar de las personas puede llegar a considerarse tecnología biométrica siempre y cuando sean recolectados y percibidos sus rasgos de una manera cuantitativa en un subconjunto de personas; y que, como característica imprescindible debe tener el caminar natural de la persona.* Pero que hay en cuanto a la definición anterior referente a la permanencia. ¿Es permanente esta tecnología? o mejor dicho ¿Por cuánto tiempo es la vida útil de un modelo en una persona antes de que el paso del tiempo repercuta en la identificación-autenticación biométrica en el sistema?

Estudios actuales se han realizado con resultados de verificaciones pobres, menores al 25% y con falsas alarmas del 1% en lapsos de tiempo alrededor de 6 meses dando como resultado a los sistemas biométricos por la manera de caminar una desalentadora imagen como tecnología biométrica permanente, pero como se explicó en nuestro trabajo, las inevitables variaciones en los rasgos conductuales deben ser usados con mecanismos de actualización de modelo para compensar los cambios sobre el tiempo, ya que la biometría por la manera de caminar es conductual, ésta debe trabajar mejor con un uso regular adaptando el modelo constantemente.

Con esto podemos concluir totalmente que la biometría por la manera de caminar de las personas puede considerarse como una tecnología biométrica.

Pero, ¿La tecnología biométrica por la manera de caminar es la más adecuada en todo momento para ser implementada? o ¿cuál debe de ser ésta?. Al igual que en la elección de los métodos de autenticación, esto depende del estudio cuidadoso de las necesidades particulares de cada usuario.

Y para establecer un estudio minucioso sobre cuál es la biometría que mejor satisface las necesidades del usuario, se deben contemplar todas y cada una de las siguientes propiedades biométricas, en nuestro caso obviamente la autenticación biométrica por la manera de caminar de las personas debe tener este estudio detallado antes de pensarse en ser implementada:

- Exactitud
- Precisión
- Velocidad computacional
- Coste
- Facilidad de uso
- Facilidad de desarrollo
- Seguridad
- Integridad
- Privacidad

Cada una de estas propiedades es analizada minuciosamente y pueden ser consultadas en el apartado 3.4 (FUNCIONAMIENTO DEL SISTEMA Y CUESTIONES DE DISEÑO).

Para completar algunas de las propiedades anteriores en nuestro estudio de la autenticación biométrica por la manera de caminar de las personas se puede mencionar lo siguiente:

- Precisión.- Debido a que la biometría por la manera de caminar de una persona es basada en su comportamiento y por lo definido ya en el apartado 3.4.2 (Precisión) la biometría por la manera de caminar tiene un índice más alto de TRF, o lo que es lo mismo, existe un índice más alto de usuarios válidos que son rechazados por error, esto debido a que existe una precisión más alta en el sistema. Por tanto, este tipo de tecnología debe ser más utilizada en aplicaciones de seguridad.
- Facilidad de uso.- Es amigable al usuario en el sentido de que ninguna otra interacción es necesaria más que el pasar por los sensores y no es necesario revelar información personal adicional más que la ya disponible. Probablemente este sea el sistema biométrico menos molesto que existiera hoy en día.
- Privacidad.- Una de las propiedades más importantes a considerar es la privacidad.

  El problema aquí es que los analistas, desarrolladores y arquitectos de sistemas; ya sea por falta de conocimientos o por una manera mal intencionada no se basan en implementar lo que realmente es la *autenticación en su manera estricta*, que como la definí al inicio del segundo capítulo es "***la verificación de tu identidad".*** Este término aunque suene muy trivial debe ser muy conciso y limitado a su propio significado; es decir, *un sistema de autenticación no debe determinar la identidad de un usuario, sino solamente debe*

confirmar su identidad; es decir, a partir de los datos almacenados en el sistema no debe ser posible por ninguna manera obtener la imagen real de una persona.

Se concluye además que el grado de variación intra-personal en las características fisiológicas es mucho más pequeño que en características conductuales. Por lo tanto, el universo de las características conductuales en una población fija a estudiar es generalmente más pequeño que para una tipología fisiológica. Por esto las propiedades anteriormente mencionadas deben ser analizadas en mayor detalle para características conductuales. Este es el caso de la tecnología biométrica por la manera de caminar de las personas.

Citemos un ejemplo, tomando como preámbulo, al balanceo de la pierna como la única característica a medir para la autenticación de la persona.

Si intentásemos medir la biometría por la manera de caminar de una persona no bastaría con tener únicamente los rasgos característicos de las piernas como una justificación suficiente para implementar esta tecnología; *ya que los rasgos característicos conductuales tendrían forzosamente que primero contar con los rasgos fisiológicos de alguna manera apta o propicia para que después el individuo pudiera caminar de una manera natural.*

No estoy diciendo con esto, que no existan variaciones intra-personales en los rasgos fisiológicos, sino trato de decir que son menos vulnerables a cambiar que los rasgos conductuales.

Tomemos el ejemplo anterior:

Con un fuerte golpe o un lapso prolongado de tiempo, los rasgos fisiológicos, en este caso la pierna, pueden llegar a ser medidos, pero puede que no pase lo mismo con los rasgos conductuales ya que son más propensos a alterar el caminar natural del individuo; inclusive golpes ajenos a la pierna o por los múltiples factores que alteran la manera del caminar y el reconocimiento de los individuos que menciono en el apartado 4.3.2.3 (Factores que alteran la manera del caminar y el reconocimiento de los individuos) pueden afectar a la autenticación del individuo.

Los estudios muestran que la biometría recae únicamente en las siguientes vulnerabilidades:

- Falsificación.- Lo cual puede ser extremadamente difícil.
- Robo.- Referente a mutilaciones en biometría fisiológica.
- Privacidad.- Invasión a la privacidad.
- Problemas con rechazos falsos o aceptaciones equivocadas.
- Cambios fisiológicos
- Características pueden ser heridas.

Y además para el caso particular del sistema de autenticación biométrico por la manera de caminar se puede consultar además el apartado 4.3.2.3 (Factores que alteran la manera del caminar y el reconocimiento de los individuos) y por supuesto leer todo este trabajo de tesis.

Por esto, el tipo de biometría conductual es suficiente cuando usamos aplicaciones de seguridad baja-a-media; porque parece ser imposible pero se han podido replicar ciertas características conductuales, como por ejemplo el patrón de la firma de un individuo; pero también una de sus principales ventajas de muchos sistemas biométricos conductuales, incluyendo a la manera de caminar de una persona es la detección de una persona viviente al momento de adquirir las muestras para ser autenticado-identificado, y con esto una característica no puede ser robada.

Por otro lado un sistema biométrico es utilizado para dos objetivos:

- **Identificación.- Determina quien una persona es**. Es una coincidencia uno-a-muchos donde el usuario no suministra su identidad. Es mayormente usado en implementaciones públicas de sistemas de seguridad.
- **Autenticación.- Determina si una persona es quien ella dice ser.** Es una coincidencia uno-a-uno donde el usuario si suministra su identidad. Es mayormente usado en instituciones privadas que tienden más hacia la autenticación.

Se puede complementar el apartado 4.3.3 (Ambientes Exteriores y Ambientes Interiores) diciendo que en circunstancias naturales (ambientes externos) existe una mayor dificultad en obtener muestras, y por tanto, un mayor nivel de dificultad en el proceso de autenticación-identificación biométrica que en circunstancias previstas (ambientes internos) debido a que hay un mayor número de

factores impredecibles (4.3.2.3 Factores que alteran la manera del caminar y el reconocimiento de los individuos)

Podemos concluir entonces, que como estamos proponiendo un sistema de autenticación biométrico y el objetivo de la autenticación en biometría es mayormente utilizado en instituciones privadas**,** los ambientes interiores deben ser mayormente implementados para este tipo de solución.

Ahora la pregunta; ¿la biometría por la manera de caminar de una persona puede ser usada tanto para verificación como para identificación?

La respuesta no es del todo precisa para la identificación y no puede ser generalizada desde que el proceso de identificación todavía no ha tenido una precisión bien definida como la explicada en el apartado 3.4.2.3. (Precisión para Identificación y para Autenticación) y por la complejidad computacional que todavía no ha podido determinar el número de usuarios que pueden ser identificados. Lo que sí podemos decir es que este tipo de tecnología es de ingresos intensivos de datos y computacionalmente cara. Además; para que una tecnología biométrica se considere útil al usuario final, la tasa de operación y la rapidez tienen que contemplar tiempos de respuesta aceptables, de 5 a 10 segundos aproximadamente para la autenticación o identificación y estas dependen del sistema de cómputo y del sensor a utilizar.

Por tal motivo, la pregunta anterior se puede responder diciendo que la identificación biometría puede ser llevada a cabo siempre y cuando el proceso de decisión proporcione resultados alrededor de 5 a 10 segundos por identificación-verificación de usuario.

Se puede entender que el módulo de identificación requiere de un mayor procesamiento que el de autenticación pero cuando el número de usuarios es pequeño estas diferencias van disminuyendo. Probablemente este tipo de tecnología en este momento no llegue a tener una tasa de error tan pequeña como la del iris para un esquema de relación 1-a-muchos, pero cabe la posibilidad de implementarla en un esquema de relación 1-a-pocos.

Si en un esquema de relación 1-a-pocos es factible implementar la identificación, en un esquema de identificación 1-a-1 o de verificación es entonces posible implementar este tipo de tecnología.

Debemos entender además, que en esta tecnología no se puede conocer que tan extensa deba ser la medida de la muestra para conocer la unicidad del biométrico; pero es importante tener en cuenta que la muestra es clave en los sistemas biométricos por la manera de caminar, pues si la muestra es demasiado grande, los tiempos de respuesta ante una decisión de reconocimiento se elevan causando la ineficiencia del sistema biométrico. Es por esta razón que los algoritmos de procesamiento para autenticación-identificación tienen que ser cada vez más eficientes proyectando medidas de modelos cada vez más pequeños, pero lo suficientemente grandes como para que no se tengan problemas al momento del reconocimiento del individuo. Se propone por ejemplo que en sistemas donde se necesiten extraer características de un ciclo por la manera de caminar, sea implementada la *simetría bilateral*, siempre y cuando la toma de la cámara hacia la persona ya se haya encontrado en una velocidad constante y no al inicio o fin del caminar de la persona, pues no se encontraría en una fase de cierre. Esto reduciría el almacenamiento en un 50% dando como resultado una respuesta más rápida en la decisión del sistema biométrico y disminuiría considerablemente el procesamiento del sistema.

Se llega a la conclusión también, que los impedimentos del reconocimiento de las personas debido a la posición de la(s) cámara(s) cada vez serán menores debido a que el estudio avanzado en los algoritmos nos llevará a obtener un reconocimiento más eficaz en el cual una o hasta varias personas caminando en cualquier ángulo o distancias lejanas a la(s) cámara(s) podrán ser reconocidas mediante ayuda de espejos, vistas canónicas, modelos en 3-D, ambientes multicámaras, otros sensores o nuevos métodos que se vayan descubriendo.

Pero hay que tener en cuenta como lo expresamos en el apartado 4.3.5 (Características a medir en el reconocimiento por la manera de caminar) que hay rasgos más importantes que otros para obtener tasas más altas de reconocimiento al medir la tecnología biométrica por la manera de caminar y que la más importante de todas es la pierna, así es que es importante que esta característica sea contemplada al momento de implementar esta tecnología y que *nunca se deben usar únicamente características estáticas (muchas de ellas del tipo cuasi-reconocimiento) para el reconocimiento por*

la manera de caminar, sino que deben servir únicamente como apoyo a las características dinámicas del reconocimiento.

En comparación a otros biométricos como el iris o la huella dactilar, la tecnología biométrica por la manera de caminar se encuentra en sus inicios. Como lo hemos mencionado, es de ingresos intensivos de datos y computacionalmente cara. Por esto, los impedimentos preliminares del surgimiento de esta tecnología fueron, la carencia de confiables, baratos y adecuados sensores, así como la falta de la miniaturización de éstos, la insuficiencia en el procesamiento del gran volumen de datos y video y el gran coste en memoria y equipo. Por todo esto, hace 15 años no hubiera sido posible implementar o estudiar a detalle este tipo de tecnología, pero ya ahora es posible y es nuestro deber seguir investigándola.

SUGERENCIAS PARA INVESTIGACIONES FUTURAS

- **Autenticación por algo que determina la posición en la Tierra**

La mayoría de las investigaciones y estudios actuales citan sólo tres métodos de autenticación, "por algo que se sabe", "por algo que se tiene" y "por algo que se es". Según Dorothy E. Denning el método de autenticación que cobrará auge en el futuro será la autenticación "por algo que determina la posición en la Tierra" entonces queda por investigar la manera en que este método de autenticación podrá ser usado en la actualidad para el mundo computacional.

- **La Privacidad**

Una de las características del funcionamiento de un biométrico y de las más importantes desde mi punto de vista es la *privacidad*. Es de suma importancia que se vayan realizando e investigando propuestas para realizar estándares para el manejo de la información en la implementación de biométricos. Dichas propuestas y soluciones deberían de contemplar:

- Naturaleza de los datos para ser mantenidos.
- Almacenamiento de los datos.
- Seguridad de los datos.
- Acceso a los datos.
- Administración de los datos.
- Derechos del usuario en consideración a los datos.

- **Facilidad de Desarrollo**

En la actualidad no existe una fácil integración en la implementación de sistemas biométricos debido a la escasez de estándares, es por eso que debido a la cada vez más rápida implementación de tecnologías biométricas en el mundo, se necesita con rapidez la creación de estándares API para la uniformidad de datos.

- **Simetría Bilateral**

Realizar más investigaciones sobre el comportamiento de la *Simetría Bilateral* en métodos que utilicen como base de estudio el ciclo del caminante.

BIBLIOGRAFÍA

Libros

[Bolle03] Bolle, R., Connel J., Pankanti S., Ratha N. y Senior A. (2003). *Guide to Biometrics*. USA: New York, Springer-Verlag.

[Boyd05] Boyd J. y Little J. (2005). *Advanced Studies in Biometrics.* Alemania: Springer Berlin/Heidelberg, pp. 19-23.

[O´Gorman04] O'Gorman L. (2004). *Guarding your Business.* USA: Avaya Labs Research, Basking Ridge, NJ, pp. 1-3, 6, 15, 19-20.

[Pfleeger96] Pfleeger, C. (1996). *Security in Computing*. USA: Upper Saddle River, NJ 07458: Prentice Hall PTR.

[Storey96] Storey N. (1996). *Safety-Critical Computer Systems*. Inglaterra: Addison Wesley Longman Limited.

[Yam01] Yam, C., Nixon M. S. y Carter J. N. (2001). *Audio- and Video-Based Biometric Person Authentication.* United Kingdom: Department of Electronics and Computer Science, University of Southampton, S017 IBJ Southampton,

Tesis

[Cattin02] CATTIN, Philippe. Biometric Authentication System Using Human Gait. Tésis (Doctor of Technical Sciences) Zürich, Swiss Federal Institute of Technology Zürich, 2002. pp. xi, 9-10, 14.

[Lewis02] LEWIS, Joseph. Biometrics for Secure Identity Verification: Trends and Developments. Tésis (Master of Science in Management Information Systems) United States of America, Univeristy of Maryland. Bowie State University, 2002. pp. 19-20.

[Rani05] RANI Sharma, Seema. LOCATION BASED AUTHENTICATION. Tésis (Maestro de Ciencias) India, Universidad de Pune, Departamento de Ciencias de la Computación, 2005. pp. ix, 1, 11-15, 20.

ISOS y Recomendaciones

[X.73692] Recomendación X.736 del CCITT (1992) | ISO/CEI 10164-7:1992, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Gestión de Sistemas: Función Señaladora de Alarmas de Seguridad.*

[X.80089]

a) ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

b) Recomendación X.800 del CCITT (1991), *Data Communication Networks: Open System Interconnection (OSI); Security, Structure and Applications.*

[X.80295] Recomendación X.802 del CCITT | ISO/CEI TR 13594:1995, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Modelo de Seguridad de Capas Inferiores.*

[X.80503] Recomendación X.805 del CCITT (2003). *Arquitectura de Seguridad para Sistemas de Comunicación Extremo a Extremo.*

[X.81096] Recomendación X.810 del CCITT | ISO/CEI 10181-1:1996, *Tecnología de la Información – Marcos de Seguridad para Sistemas Abiertos: Visión General.*

[X.81296] Recomendación X.812 del CCITT | ISO/CEI 10181-3:1996, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Marcos de Seguridad para Sistemas Abiertos: Marco de Control de Acceso.*

[X.81397] Recomendación X.813 del CCITT | ISO/CEI 10181-4:1997, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Marcos de Seguridad en Sistemas Abiertos: Marco de No Rechazo.*

[X.81496] Recomendación X.814 del CCITT | ISO/CEI 10181-5:1996, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Marcos de Seguridad para Sistemas Abiertos: Marco de Confidencialidad.*

[X.81596] Recomendación X.815 del CCITT | ISO/CEI 10181-6:1996, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Marcos de Seguridad para Sistemas Abiertos: Marco de Integridad.*

[X.81695] Recomendación X.816 del CCITT (1995) | ISO/CEI 10164-8:1993, *Tecnología de la Información – Interconexión de Sistemas Abiertos – Marcos de Seguridad para Sistemas Abiertos: Marco de Auditoría y Alarmas de Seguridad.*

[X.84101] Recomendación X.841 del CCITT | ISO/CEI 15816:2001, *Tecnología de la Información – Técnicas de Seguridad – Objetos de Información de Seguridad para Control de Acceso.*

Documentos Electrónicos

[Denning05] DENNING, D. and MACDORAN, P. *Location-Based Authentication: Grounding Cyberspace for Better Security.* [En línea]: Documuento electrónico cuyo origen es Internet. 1996. [fecha de consulta: 23 Junio 2005] Computer Fraud & Security, 1996. Disponible en: http://www.cosc.georgetown.edu/~denning/infosec/Grounding.txt.

[Markowitz05] J. MARKOWITZ CONSULTANTS The Human Side of Computing. *Frequently asked questions. What is the difference between speaker verification and voice authentication* [En línea]: Documuento electrónico cuyo origen es Internet. [fecha de consulta: 12 Septiembre 2005]. Disponible en: http://www.jmarkowitz.com/ask.html.

[Towson05] TOWSON UNIVERSITY. *Global Positioning System* [En línea]: Documento electrónico cuyo origen es Internet. [fecha de

consulta: 4 Agosto 2005]. Disponible en: http://tiger.towson.edu/users/nsharm1/gps.htm.

[Webopedia07] WEBOPEDIA The encyclopedia dedicated to computer technology. *Biometrics* [En línea]: Documento electrónico cuyo origen es Internet. [fecha de consulta: 6 Enero 2007]. Disponible en: http://webopedia.internet.com/TERM/B/biometrics.html.

Documentos y otras Publicaciones Científicas

[Barclay78] C. Barclay, J. Cutting and L. Kozlowski. *Temporal and spatial factors in gait perception that influence gender recognition. Perception and Psychophysics 23* (1978), pp. 145-152.

[Barron94] J. Barron, D. Fleet and S. Beauchemin. *Performance of optical flow techniques.* International Journal of Computer Vision 12 (1994), pp. 43-77.

[Baumberg93] A. Baumberg and D. Hogg. *Learning flexible models from image sequences.* Techincal report 93.36, University of Leeds School of Computer Studies 1993.

[Baumberg95] A. Baumberg and D. Hogg. *Learning spatiotemporal models from training examples.* In: British Machine Vision Conference, Birmingham 1995.

[Ben-Abdelkader01] C. Ben-Abdelkader, R. Cutler, H. Nanda and L. Davis. *Eigengait: motion-based recognition of people using image self-similarity.* In: Audio- and Video-Based Biometric Person Authentication, Halmstad, Sweden, 2001.

[Ben-Abdelkader02] C. Ben-Abdelkader, R. Cutler, L. Davis. *Person identification using automatic height and stride estimation.* In: 16th International Conference on Pattern Recognition, Quebec, Quebec 2002, pp. 377-380.

[Ben-Yacoub99] S. Ben-Yacoub, Y. Abdeljaoued and E. Mayoraz. *Fusion of FACE and Speech Data for Person Identity Verification* Dalle Molle Institute for Perceptual Artificial Intelligence 1999, pág 11.

[Bertenthal93] B. Bertenthal and J. Pinto. *Complementary processes in the perception and production of human movements.* A Dynamic Systems Approach to Development: Applications. MIT Press, Cambridge, MA 1993, pp. 209-239.

[Bhanu02] B. Bhanu and J. Han. *Bayesian-based performance prediction for gait recognition.* In: IEEE Workshop on Motion and Video Computing, Orlando, Florida 2002, pp. 145-150.

[Bissiacco01] A. Bissacco, A. Chiuso Y. Ma and S. Soatto. *Recognition of human gaits.* In: Computer Vision and Pattern Recognition 2001.Volume II., Kauai, HI 2001, pp 52-57.

[Bobick01] A. Bobick and A. Johnson. *Gait recognition using static activity-specific parameters.* In: Computer Vision and Pattern Recognition 2001. Volume I., Kauai, HI 2001, pp. 423-430.

[Boyd03] J. Boyd. *Synchronization of oscillations for machine perception of gait.* In review 2003.

[Bregler97] C. Bregler. *Learning and recognizing human dynamics in video sequences.* In: Computer Vision and Pattern Recognition 1997, San Juan, Puerto Rico 1997, pp. 568-574.

[Bregler98] C. Bregler and J. Malik. *Tracking people with twists and exponential maps.* In: Computer Vision and Pattern Recognition 1998, Santa Barbara 1998.

[Cherry04] K. Cherry. *Biometrics: An In Depth Examination.* SANS Institute 2004, pág. 3.

[Cohen00] L. Cohen, T. Shipley, E. Marshark, K. That and D. Aster. *Detecting Animals in point-light displays.* In: Twenty Second Annual Meeting of the Cognitive Science Society, Philadelphia, PA 2000, pág. 70.

[Cunado95] D. Cunado, J. M. Nash, M.S. Nixon, and J. N. Carter. *Gait extraction and description by evidence-gathering.* In Proc. Int. Conf. Audio and Video Based Biometric Person Authentication 1995, pp. 43-48.

[Cunado99] D. Cunado, M. Nixon and J Carter. *Gait Extraction and Description by Evidence Gathering.* 2nd Int. Conf. on Audio and Video-Based Biometric Person Authenticartion 1999.

[Cunado03] D. Cunado, M. Nixon and J. Carter. *Automatic extraction and description of human gait models for recognition purposes.* Computer Vision and Image Understanding 90 (2003), pp. 1-41.

[Cutting77] J. Cutting and L. Kozlowski. *Recognizing friends by their walk: gait perception without familiarity cues.* Bulletin of the Psychonomic Society 9 (1977), pp. 353-356.

[Cutting97] J. Cutting and L. Kozlowski. *Recognizing the sex of a walker from a dynamic point-light display. Perception and Psychophysics 21* (1997), pp. 575-580.

[Daugman02] J. Daugman. *How Iris Recognition Works.* IEEE Conf. on ICIP 2002.

[Davis97] J. Davis and A. Bobick. *The representation and recognition of action using temporal templates.* In Computer Vision and Pattern Recognition (CVPR) 1997.

[Davis99] J. Davis. *Recognizing Movement using Motion Histograms.* Tech. Rep. 487, MIT Media Laboratory 1999.

[Donn91] B. Donn. *An Essay: Restarting the Foundations of Information Security ISP News* May/Jun 1991, pp. 139-151.

[Dunker04] M. Dunker. *Don't Blink. Iris Recognition for Biometric Identification.* SANS Institute 2004, pp. 7, 9.

[DWilliams02] D. Williams. *A Concept for Universal Identification.* SANS Institute 2002, pág 9.

[Faúndez98] M. Faúndez. *Aplicaciones de la verificación biométrica*. Escuela Universitaria Politécnica de Mataró 1998, pág. 1.

[German04] K. German, B. Simon, H. Jessica and K. Takeo. *Markerless Human Motion Transfer*. Robotics Institute, Carnegie Mellon University, Pittsburgh PA 15213. (2004).

[Graham03] D. Graham. *It's All About Authentication.* SANS Institute 2003, pág. 5.

[Green06] R. Green and L. Guan. *Quantifying and Recognizing Human Movement Patterns from Monocular Video Images – Part II: Applications to Biometrics* 2006, pág. 112.

[Gross01] R. Gross and J. Shi. *The cmu motion of body (mobo) database.* Technical Report CMU-RI-TR-01-18. Robotics Institute, Carnegie Mellon University 2001.

[GWilliams02] G. Williams. *More than pretty face, Biometrics and SmartCard Tokens.* SANS Institute 2002, pp. 1, 3.

[Hay04] R. Hay. *Physical Security: A Biometric Approach*. SANS Institute 2004, pág. 1.

[Huang99] P. S. Huang, C.J. Harris and M.S. Nixon. *Recognizing humans by gait via parametric canonical space.* Artif. Intell. Eng., vol. 13, no. 4, Oct 1999, pp. 359-366.

[Hunter97] E. A. Hunter, P.H. Kelly and R.C. Jain. *Estimation of articulated motion using kinematically constrained mixture densities.* In: Nonrigid and Articulated Motion Workshop, San Juan, Puerto Rico 1997.

[Jain04] A. Jain, A.Ross, S. Prabhakar. *An Introduction to Biometric Recognition.* IEEE Transactions, Vol. 14. No. 1 January 2004, pp. 2, 6, 9-10.

[Johansson73]G. Johansson. *Visual perception of biological motion and a model for its analysis. Perception and Psychophysics* 14 (1973), pp. 201-211.

[Johansson75]G. Johansson. *Visual motion perception.* Scientific American 1975, pp. 76-88.

[Jonathon57] P. Jonathon, A. Martín, C. Wilson and M. Przybocki. *An Introduction to Evaluating Biometric Systems.* National Institute of Standards and Technology 2000, pág 57.

[Kale03] A. Kale, K. Amit, C. Roy and C. Rama. *Towards a View Invariant Gait Recognition.* Algorithm Center of Automation Research. University of Maryland College Park, MD 20742 July 2003, pp. 1, 6-7.

[Kale04] A. Kale, A. Sndaresan, A.N. Rajagopalan, N. P. Cuntoor, K. Amit, Roy-Chowdhury, V. Krüger and R. Chellappa. *Identification of Humans Using Gait.* IEEE Transactions on Image Proccessing, Vol. 13, No. 9, September 2004, pp. 1163, 1165, 1167, 1170.

[Laszlo96] J. Laszlo, M. van de Panne and E. Fiume. *Limit cycle control and its application to the animation of balancing and walking.* In SIGGRAPH 96 (1996), pp. 155-162.

[Little98] J. Little. and J. Boyd. *Recognizing people by their gait: the shape of motion. Videre 1* (1998). Journal of Computer Vision

Research. Quarterly Journal, The MIT Press. Volume 1, Number 2. Winter 1998, pp. 1-32.

[Liu98] F. Liu and R.W. Picard. *Finding periodicity in space and time.* In: International Conference on Computer Vision 1998.

[Liu04] Z. Liu and S. Sarkar. *Outdoor Biometrics over Time by Fusing Gait with Face.* Computer Science and Engineering University of South Florida, Tampa, Florida 33647 (2004), pág. 1.

[Murray64] M. Murray, A. B. Drought, R. Bernard Kory. *Walking paterns of normal men.* The journal of Bone and Joint Surgery 46A 1964, pp. 335-360.

[Murray67] M. Murray. *Gait as a total pattern of movement.* American Journal of Physical Medicine, vol. 46(1). ISSN 0002-9491. February 1967, pp. 290-333.

[Myers02] L. Myers. *An Exploration of Voice Biometrics*. SANS Institute 2002, pp. 3, 5, 9.

[Naresh03] C. Naresh, A. Kale, C. Rama. *Combining multiple evidences for gait recognition.* Center for Automation Research. University of Maryland at College Park MD 20742 USA 2003.

[Nixon99] M.S Nixon, J.N. Carter, D. Cunado, P.S. Huang and S.V. Stevenage. *Automatic Gait Recognition.* University of Southampton, Southampton UK 1999, pág. 1.

[Olsson03] T. Olsson. *Strengthening Authentication with Biometric Technology.* SANS Institute 2003, pp. 2-5.

[Pankanti00] S. Pankanti, R. Bolle and A. Jain. *Biometrics: The Future of Identification. IEEE* 2000, pp. 46-49.

[Penny02] W. Penny. *Biometrics: A Double Edged Sword – Security and Privacy.* SANS Institute 2002, pp. 1, 3, 5.

[Phillips00] J. Phillips, A. Martin, C. Wilson and M. Przybocki. *An Introduction to Evaluating Biometric Systems.* IEEE Computer, Vol. 33(2): February 2000, pp. 56-63.

[Phillips02] P. J. Phillips, S. Sarkar, I. Robledo, P. Grother and K. Bowyer. *The gait identification challenge problem: Data sets and baseline algorithm.* In International Conference on Pattern Recognition 2002, pp 385-388.

[Phillips03] P. J. Phillips, G. Patrick, J. M. B. Duane, T. Elham and B. Mike. *Face recognition vendor test 2002.* Technical report, NISTIR6965: www.frvt.org, March 2003.

[Poana98] R. Polana and R. Nelson. *Detection and recognition of periodic, non-rigid motion.* International Journal of Computer Vision 23 (1998).

[Rowler97] H.A. Rowley and J. M. Rehg. *Analyzing articulated motion using expectation-maximization.* In: Computer Vision and Pattern Recognition 97, San Juan, Puerto Rico 1997, pp. 935-941.

[Sarkar02] S. Sarkar, J. P. Phillips, I. Robledo, P. Grother, y K. W. Bowyer. *Baseline Results for the Challenge Problem of Human ID Using Gait Analysis.* To appear at 5th IEEE International Conference on Automatic Face and Gesture Recognition May 2002.

[Schmidt00] C. Schmidt. *Der bewegte Mensch.* Magazin für Computer Technik c't, vol. 23: 2000, pp 118-122.

[Shutler01] J. Shutler and M. Nixon. *Zernike velocity moments for description and recognition of moving shapes.* In: British Machine Vision Conference 2001, Manchester, UK Session 8: Modelling Behaviour 2001.

[Spencer02] N. M. Spencer and J. N. Carter. *Viewpoint Invariance in Automatic Gait Recognition.* Image, Speech and Intelligent Systems. University of Southampton, UK 2002.

[Stewart99] I. Stewart. *Symmetry-breaking cascades and the dynamics of morphogenesis and behaviour*. Sc. Progress, 82(1) 1999, pp. 9-48.

[Tanawongsuwan01] R. Tanawongsuwan and A. Bobick. *Gait recognition from time-normalized joint-angle trajectories in the walking plane*. In: Computer Vision and Pattern Recognition 2001. Volume II, Kauai, HI 2001, pp. 726-731.

[Von03] T. Von and B. Goepfert. *Gender dependent EMGs of runners resolved by time/frequency and principal pattern analysis.* Journal of Electromyography and Kinesiology 13 (2003), pp. 253-272.

[Wachter97] S. Wachter, H. H. Nagel. *Tracking of persons in monocular image sequences.* In: Nonrigid and Articulated Motion Workshop, San Juan, Puerto Rico 1997.

[Wang02] L. Wang, H Ning, W. Hu and T. Tan. *Gait Recognition based on Procrustes Shape Analysis.* Liang National Laboratory of Pattern Recognition. Institute of Automation, Chinese Academy of Sciences, Beijing, P.R. China, 100080 2002, pág. 1.

[Wren97] C. Wren, A. Azarbayenjani, T. Darrell and A.P. Pentland. *Pfinder: real-time tracking of the human body.* IEEE Transactions on Pattern Analysis and Machine Intelligence 19 (1997), pp. 780-775.

[Zeg02] S. Zeg. *Biometric Technology Stomps Identity Theft.* SANS Institute 2002, pág. 6.

[Zimmerman02] M. Zimmerman. *Biometrics and Users Authentication*. SANS Institute 2002, pp. 2-3.