Tecnologías Biométricas aplicadas a la seguridad en las organizaciones

Mg. Luzmila Pró[1], Mg. Juan Carlos Gonzáles[1], Lic. Walter Contreras[1] , Lic. Carlos Yañez[1]

[1]Facultad de Ingeniería de Sistemas e Informática
Universidad Nacional Mayor de San Marcos

lproc2003@hotmail.com, jgonzales@unmsm.edu.pe, wcontrerasf@unmsm.edu.pe, cyañez d@unmsm.edu.pe

RESUMEN

El presente estudio trata sobre la biometría y sus aplicaciones en nuestro medio. La biometría informática, actualmente, es una de las ciencias más importantes. Últimamente existen aplicaciones y estudios de investigación, pero sin embargo todavía hay mucho por investigar por cuanto existen muchas aplicaciones relacionadas, una de ellas es la seguridad. En los últimos años la demanda de los sistemas biométricos se ha incrementado debido a que la reputación y seguridad en las organizaciones de la sociedad del conocimiento se hace cada vez más vulnerable ocasionando pérdidas económicas cuantiosas, así como en otros aspectos del ser humano.

La seguridad es un aspecto de vital importancia que tanto el gobierno como las organizaciones deberían tomar cartas en el asunto a fin de que corporativamente realicen cada uno en su ambiente el control físico de las personas que ingresan a las instalaciones así como también en lo que respecta a la seguridad de la información.

En el presente estudio es una investigación teórica asimismo la evaluación de las aplicadas a la seguridad en las organizaciones y la propuesta de un modelo de implantación de control de asistencia de personal administrativo y docente en la Facultad de Ingeniería de Sistemas e Informática aplicando las Tecnologías Biométricas.

Palabras clave: Tecnologías biométricas, seguridad, organizaciones, vulnerabilidad, identificación, verificación, alineamiento

ABSTRACT

The present study to treat on the Biometry and the applications in our environment.

The Informatic biometry, in the present time is considerate a sciences more import ants, the ultimate existing applications and studies of investigation, but nevertheless even exist themes as security for to investigate.

In the last years the demand of the biometrics systems to increase oneself owing a the reputation and security in the organizations of knowledge society is more and more vulnerability and that cause danger and quantity economics loss, so that in the others aspects of to be human.

The security is one aspect vital of importance that the government as the organizations to have obligation to se corporative to realice each one in their environment the physical control of the persons what enter to into of the installations as also the informatics security.

The present study is theoretical investigation thus same the evaluations of the applications at the security in the victuals organizations and the propose of the Model on the implementation of the personnel control in the Engineer Of Systems and Informatics Faculty, applications of the biometrics technology.

Keywords: Biometrics technology, Security, organizations, vulnerability, identification, verification storage.

INTRODUCCIÓN

El presente estudio trata sobre la biometría y sus aplicaciones en nuestro medio.

Se eligió tecnologías biométricas con tecnologías de seguridad por ser ambos muy de actualidad y que en nuestro medio aún no existen investigaciones realizadas al respecto sobre todo tratándose de organizaciones.

El aspecto de seguridad considera este estudio que es de vital importancia que tanto el gobierno como las organizaciones deben participar en esta labor, a fin de que corporativamente se cuenten con herramientas que posibiliten la seguridad tanto en el acceso a los sistemas informativos así como el control físico de las personas en cuanto al acceso a las instalaciones. En el presente estudio se han realizado los siguientes:

- Investigación teórica, tanto de la Tecnología Biométrica (TB) como de las Tecnologías de Seguridad (TS), sus antecedentes y sus aplicaciones.

- Evaluación de las diversas aplicaciones de Tecnólogas Biométricas y de Tecnologías de Seguridad, asimismo se diseñarán algoritmos de identidad y registro, seleccionando las tecnologías más apropiadas.

- Análisis de los diversos estudios de la biometría tanto estática como dinámica y sus aplicaciones y propuesta del modelo de control de asistencia del personal administrativo y docente para la Facultad de Ingeniería de Sistemas e Informática.

1. FUNDAMENTACIÓN TEÓRICA

1.1 Conceptos Básicos

Biometría.

A la biometría se le define como la ciencia dedicada al estudio estadístico de las características cuantitativas de los seres vivos como son: peso, longitud, etc. Este término es utilizado para referir a los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas. [TAPIADOR, 2005]

La biometría se encuentra vinculada también al área de la criptografía y seguridad informática, así estas tres áreas pueden considerarse como los pilares para la concepción de un sistema de seguridad aplicando tecnologías biométricas en las organizaciones, por ejemplo, algo que una persona en estos tiempos debe saber es su clave secreta si desea acceder a su cuenta bancaria, para realizar una transacción, tiene una tarjeta personal, y a la vez es una persona a quien se le puede identificar biométricamente, por ejemplo mediante su huella dactilar.

En función de las características que se usan en la identificación se distinguen dos áreas:

- **Biometría estática**: Es el estudio de las características físicas del ser humano.

- **Biometría dinámica:** Estudia las características de la conducta del ser humano.

A la biometría estática pertenecen las características: huella dactilar, ojo, retina, iris, líneas de la mano, geo-

metría de la mano, geometría facial, características de la cara, poros de la piel, etc.

A la biometría dinámica pertenecen las características: manuscrito, firma, voz, tecleo, gestos o movimiento corporal. [1DW]

Para que las características físicas y conductuales sean utilizadas como elementos de identificación deben cumplir con los siguientes requisitos:

a). Universalidad: Todas las personas tienen o presentan una característica.

b). Singularidad: Dos personas cualesquiera son distinguibles una de la otra en base de sus características.

c). Estabilidad: La característica tiene que ser lo suficientemente estable a lo largo del tiempo y en condiciones ambientales diversas.

d). Cuantificable: La característica tiene que ser mesurable cuantitativamente.

e). Aceptabilidad: El nivel de aceptación de la característica por parte de las personas debe ser suficiente como para ser considerada parte del sistema de identificación biométrico.

f). Rendimiento: El nivel de exactitud requerido debe ser elevado para que la característica sea aceptable.

g). Usurpación: Permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas.

El objetivo de usar características biométricas es poseer un conjunto de herramientas que permitan obtener la identificación y verificación de la identidad de una persona.

1.2 Identificación y Verificación

1.2.1 Identificación

Identificación se refiere a que mediante un sistema biométrico, se trata de responder a la pregunta: **¿Quién es la persona X?**, se tiene la información de la persona de la que se desconoce su identidad, para ello se debe contar con un sistema que disponga de los siguientes elementos: [TAPIADOR, 2005]

- Base de datos: almacene las características biométricas de una gran cantidad de personas, como por ejemplo la base de datos de la RENIEC.
- Un mecanismo para capturar y procesar las características biométricas de las personas a identificar.
- Un procedimiento para comparar las características de las personas a identificar con las almacenadas en la base de datos y que permita tomar decisiones de responder a la pregunta formulada. El tipo de comparación es de uno a muchos (1:N).

1.2.2 Verificación

El sistema biométrico trata de responder a la pregunta: **¿Es esta persona X?**, es decir una persona reclama tener una identidad y el sistema debe verificar la determinada identidad acerca de su certeza, para ello es necesario contar con un sistema que disponga de los siguientes elementos: [TAPIADOR, 2005]

- Un sistema de identificación tipo usuario más password al que se le puede añadir un identificador como un documento de identidad, ejemplo documento nacional de identidad o su código de trabajo.
- Un mecanismo para capturar y procesar las características biométricas de la persona a identificar.
- Un procedimiento para comparar las características de la persona a identificar con la que se ha almacenado previamente para esta persona y que permita tomar la decisión de contestar a la pregunta formulada, es una comparación uno a uno (1:1).

1.3 Antecedentes de la biometría

El siguiente es un resumen de los antecedentes más saltantes de la biometría: [1DW]

En el siglo VIII, en China se encontraron huellas dactilares, en documentos, y en trabajos de arcilla.

En el año 1000, Quintiliano utilizó las huellas dejadas por las palmas de la manos ensangrentadas para esclarecer un crimen.

En 1686, Marcelo Malpigio hizo un primer estudio de sistemático de huellas dactilares.

En 1856, Sir William Herschel, implanta la huella de dedo pulgar, como método de identificación en documentos para personas analfabetas.

En 1880, Henry Faulds, médico escocés en Tokio, publicó un artículo en la Revista Nature, sugería que la huellas dactilares encontradas en la escena de un crimen podían identificar al verdadero culpable.

En 1930, en la Universidad de Harvard desarrollan Algoritmos para el Reconocimiento Biométrico a través del patrón de iris.

En 1941, Murria Hill en los Laboratorios Bell, inicia el estudio de identificación de voz.

En 1950: Convierte: escritura humana a texto digital usando Dispositivo Optical Carácter Recognition (OCR).

En 1960: Reconocimiento y Autenticación de una persona a través de la mano.

En 1994: En EEUU se usan técnicas de reconocimiento de patrones y redes neuronales artificiales desarrollados en lenguaje Assembler y Fortran.

En 1986: Alec Jeffreys utilizó por primer vez el ADN para identificar al autor de unos asesinatos en Inglaterra.

En 1989: El National Institute Standards and Technology de EEUU comenzó a desarrollar métodos para probar sistemas biométricos.

En 1994: Patente de algoritmos sobre reconocimiento de patrón de iris.

En 1996: Sensor Corp. lanza al mercado una cámara especial para adquirir imágenes de iris en cajeros automáticos, luego se difunde en varios países de Europa.

En 1997: IEEE dedica un número especial: Proceddings de Automatización Biométrica.

En 1998, se constituye el consorcio Bio API para desarrollar un API ampliamente aceptado y disponible que sirva para las diversas tecnologías biométricas.

En 2002: Universidad de Torino: Mejora el rendimiento de seguridad basados en dinámica de tecleo.

1.4. Relación del cuerpo humano y la biometría

En el área de la biometría el cuerpo humano es fundamental incluyendo sus características físicas y conductuales, y que son útiles la identificación y verificación.

La biología es la ciencia que estudia dos tipos de características al observar un individuo (s) como son:

- Características externas o fenotipo son las que estudia la Biometría
- Características genéticas o genotipo son las que estudia la Genética

El cuerpo humano posee una estructura funcional y sus características pueden estudiarse desde diferentes niveles de complejidad organizativa conocida como niveles de organización y que abarcan desde su composición química, biofísica a la conductual, pasando por una serie de niveles organizativos de complejidad crecientes como son las células, los tejidos, los órganos y los sistemas. [CLARKE, 1994].

La biometría, ante la gama de características que ofrece el cuerpo humano, se pueden aplica a diversos estudios, ejemplo los relacionados con la seguridad, identificación de las personas. Las características de los seres humanos medibles y susceptibles de usar en la biometría se pueden dividir en dos grupos:

1. Características estructurales: Se encuentran vinculadas a determinados órganos y sistemas, por ejemplo el sistema óseo, muscular (cara, las manos), ojos, la retina, iris, la piel, las huellas dactilares.
2. Características de tipo funcional: las características consideran el aspecto de movimiento corporal, ejemplo el tecleo, el manuscrito, movimiento de la boca en el caso del habla o reconocimiento de voz.

1.5 Relación de la Biometría y la Seguridad

La biometría actualmente es una de las tecnologías que se está usando en la seguridad, para la identificación, por ejemplo el control al acceso a un banco para realizar transacciones bancarias, o para transacciones de compra, venta en los negocios con puntos de venta mediante tarjetas de crédito. Pero, el problema es que la seguridad se puede ver vulnerada con este tipo de identificación del usuario. La biometría nos muestra otra opción de contraseña o para poder identificar al usuario. (Nadler, 1993)

2. MÉTODOS Y MODELOS

2.1. Modelo de la Tecnología Biométrica:

La tecnología biométrica es un sistema que consiste de cinco subsistemas: recopilación de datos, transmisión de datos, procesamiento de señales, almacenamiento de datos, toma de decisión y evaluación y rendimiento

a) La recopilación de datos: Es un subsistema encargado de la captación de datos, abarca los aspectos desde la fase de darse alta en el sistema como en los procedimientos de identificación y verificación que se lleva a cabo cuando un usuario pretende acceder a un sistema controlado mediante técnicas biométricas. Entre los problemas que pueden surgir en esta etapa se encuentran los re-

ferentes a la variabilidad de la información por los siguientes aspectos:

- Las medidas biológicas están sujetas a deterioro (edad y otros, accidentes u heridas, traumas, etc.).
- El uso de dispositivos físicos que se encargan de la captación de datos, mediante sensores, entendiéndose, que la información a captar sea de la forma mas estandarizada posible, por ejemplo en la medición de la cara frente a la cámara tomar en cuenta la posición estándar, igual para el caso de una toma de huella dactilar, también dependen del dispositivo (calibración, la calidad y grado de estabilidad o sensibilidad, aspectos como deterioro del equipo, el ambiente (iluminación y otros).

b) La transmisión de datos: Generalmente la captación de datos se suele realizar fuera del lugar donde se va a almacenar.

Las mediciones biométricas, en general, ocupan gran cantidad de espacio de almacenamiento debido a la naturaleza de la información captada, como pueden ser: imágenes del rostro, huellas dactilares, voz o sonido de video, etc.

Esta problemática de tener un volumen de información considerable se suele agrupar en dos aspectos:

- Sistemas de compresión estándar no necesariamente vinculados a datos biométricos, es común utilizar para ello algoritmos JPEG para comprimir imágenes y la predicción lineal para el sonido FPS 1014.
- Para casos especiales de captación de datos biométricos existen dispositivos especialmente diseñados, por ejemplo para huella dactilar. Se utilizan algoritmos de cuantificación escalar mediante Wavelets.

La transmisión de información presenta problemas como ruido, caso de señales analógicas.[JAIN, 1997]

c) Procesamiento de señales: La información que proviene del subsistema anterior es transformada en el siguiente subsistema mediante algoritmos, que extraen las características biométricas presentes en la señal original y que debido a sus propiedades invariantes al tiempo, a la forma de presentación al tipo de sensores, al método de comprensión y al sistema de transmisión se consideran como las más relevantes a efectos de comparación entre diferentes muestras.

Generalmente la información a procesarse se manipula mediante vector de características, en casos como huellas y imágenes faciales la información es recopilada / procesada en matrices.

d) Almacenamiento de información: La información del proceso de tecnología biométricas se almacena mediante plantillas o patrones o templates en una base de datos, mediante tokens portátiles como por ejemplo un smart card.

e) Toma de decisión: El proceso de identificación y verificación finaliza con la medida de un índice de comparación entre los patrones almacenados y los datos que ingresa el usuario cuando accesa al sistema, este índice permite tomar decisión sobre la identificación y verificación si es satisfactoria o no.

f) Evaluación y rendimiento: Los sistemas de evaluación y medida de rendimiento en las aplicaciones biométricas permiten establecer criterios objetivos que ayudan a la comparación entre diferentes productos, este tipo de evaluación es costosa dado que se realiza de manera exhaustiva: análisis de datos, extraer conclusiones, elaborar documentación pertinente, asimismo se deben realizar pruebas de objetividad e independencia necesaria tal que se asegure los criterios válidos que sean aceptados por los fabricantes implicados en el desarrollo de soluciones mediante la biometría.

2.2. Evaluación de Sistemas Biométricos:

La evaluación de un sistema biométrico consiste en evaluar diferentes aspectos que incluye desde la adquisición de los datos a la integración del sistema. [PHILLIPS, 2000].

Entre los puntos más saltantes que analizan son:

- El rendimiento con respecto a la función (reconocimiento automático de personas).
- La seguridad, integridad y confidencialidad de los datos que maneje el sistema.
- La fiabilidad, disponibilidad y mantenimiento de la aplicación informática.
- La comercialización del producto, la estimación de los costos y beneficios.
- La aceptación y la facilidad de manejo por parte del usuario.
- El aspecto legal, dado que trata con temas relacionados a la seguridad y privacidad de personas.

La evaluación es un proceso que requiere conocimiento de los siguientes conceptos:

- Muestra: Es el resultado de la captación de datos por el sensor correspondiente a un determinado rasgo biométrico, ejemplo la señal de voz adquirida por un micrófono, la imagen de una huella dactilar, la cara, o el iris son muestras.
- Patrón o Template: Es la medida de referencia almacenada en una base de datos de los usuarios, obtenida a partir de muestras de entrenamiento proporcionado por este, su clasificación se realiza a través de vectores de características extraídos de las muestra de entrenamiento, en este proceso se usan algoritmos como: Técnica de los K-vecinos más próximos sin agrupamiento de vectores, Parámetros de un modelo creado / entrenado a partir de esos vectores, pesos en una red neuronal, probabilidades relacionados al modelo oculto de Markov.
- Inscripción: Es el proceso de añadir un nuevo usuario al sistema, incluye la operación de crear.
- Operación: El usuario puede identificar/validar su identificación según política de decisión establecida.

2.2.1. Clasificación de la Muestra:

Evaluar un sistema requiere de muestras tanto para crear patrones de referencia como para realizar las pruebas, se puede, distinguir los siguientes modos:

Online: La clasificación es durante la captura de la muestra. No hay almacenamiento.

Offline: La clasificación y las pruebas se realizan con muestras previamente grabadas. La creación de bases de datos permite un mayor control y versatilidad de las pruebas que se realizan sobre el sistema con un costo mínimo, las características de evaluación son modificables. [PHILLIPS, 2000]

2.2.2 Tipos de Evaluación:

Se pueden distinguir tres tipos de evaluación:

a) Evaluación de la Tecnología: Es en modo offline y repetitivo, se busca medir la tecnología, determinar el proceso, identificar los enfoques más objetivos, se obtienen en laboratorios independientes con base de datos estándar. Las bases de datos no deben ser conocidas por los grupos participantes.
b) Evaluación de Escenario: Mide el rendimiento del prototipo a fin de determinar si la tecnología está acorde a los requisitos de funcionamiento, incluye algoritmos, sensores, personas que van a manipular:
c) Evaluación Operacional: Es similar al de escenario pero se realiza con datos reales y para una población determinada. El objetivo es analizar si el sistema biométrico cumple con los requisitos de una determinada aplicación. Puede ser online o en offline.

2.3. Biometría Estática

La identificación de una persona es muy importante en seguridad informática y en seguridad en general, mediante la biometría estática se podrá identificar a una persona por sus características como huella dactilar, iris, retina, geometría de la mano y otras.

La biometría es un área muy amplia, se ha seleccionado la biometría estática y en particular la huella dactilar, a continuación explicamos:

2.3.1. Huella dactilar:

Huella dactilar o *fingerprint* en inglés, es una característica biométrica de tipo morfológico, la huella dactilar se basa en la presencia de un conjunto de líneas genéricas llamadas ***crestas,*** son partes donde la piel se eleva sobre las zonas más bajas (valles), siendo el ancho de los valles de 2 a 5 décimas de milímetro [LIN, 1998].

La huella dactilar en los seres humanos se manifiesta a partir del sexto mes de desarrollo del embrión como consecuencia de un proceso aleatorio, por lo que se puede afirmar que no existe ningún tipo de correlación entre gemelos idénticos o individuos de una misma familia, son invariables con el tiempo, el dibujo papilar crece proporcionalmente según el desarrollo físico corporal, sin alterar el número, el grado de curvatura, ni la situación de las crestas presentes en la misma, por tanto una modificación es difícil tanto fisiológica, voluntaria o patológicamente, son por tanto características invariantes, propias y unívocas del individuo. La captación de huellas dactilares presenta algunas dificultades en la toma de muestras para su procesamiento:

- De tipo étnico: Las huellas de los asiáticos presentan crestas muy pequeñas y finas, esto dificulta la captación de huellas dactilares.
- De tipo profesional: gente que labora con las manos, en general presentan callosidades (albañiles, carpinteros o que usan productos químicos de na-

turaleza corrosiva),dificulta la captura de huellas dactilares.

- Las crestas presentan dos características particulares denominadas minucias:
- *Final de cresta*: característica es el punto en que la cresta se acaba de forma abrupta.
- *Bifurcación de la cresta:* es el punto en que la cresta se bifurca en dos o mas crestas.

Estas dos características quedan unívocamente definidas a partir de su localización (coordenadas X e Y) respecto del sistema de coordenadas central de la imagen y orientación en un ángulo θ, las primeras responden a un 68% del total de las minucias presentes en una huella, mientras que las segundas contabilizan el 32% restante. El número de minucias en una huella dactilar es de 40 y 100. Otras singularidades que se presentan en una huella dactilar son: *Core y Delta.*

Core: Situado en el centro (núcleo de la huella) aquí se unen las crestas y cambia bruscamente su dirección, describe un ángulo de 180 grados, retornando a la posición de origen. Este punto es usado como punto de referencia a partir del cual se cuentan el número de crestas a considerar en un análisis dactiloscópico.

Delta: Es un punto característico del dibujo papilar de algunas huellas dactilares que pueden presentarse en forma de triángulo, formado por la aproximación o fusión de crestas existentes en la zona frontera (marginal, basilar y nuclear) de la huella.

Para efectuar mediciones mediante huella dactilar [LIN, 19988] se requiere de:

1. **Algorítmica:** La algorítmica asociada a la clasificación de huellas dactilares se presenta a un nivel aceptable de discriminación entre clases (distancia interclase) y es un poco sensible a las variaciones que produce en las diferentes realizaciones de una misma clase (distancia intraclases). Las interclases e intraclases reales resultantes de la configuración de los patrones globales así como la baja calidad de las imágenes originales hacen que esta etapa de clasificación sea un problema de elevada complejidad.
2. **Dispositivos de captura de huellas dactilares:** En la actualidad, existen una variedad de dispositivos de captura de huella dactilar. Estos dispositivos son del tipo *inkless (*captura de huellas y su uso):

- Lectores OEM: Son de solución discreta, se integran a sistemas electrónicos.
- Lectores integrados: Son dispositivos de captura de huellas y se conectan a un computador mediante el puerto USB, almacenan los datos generados en disco duro.
- Terminales completos de Identificación: Dispositivos que incorporan hardware y software necesario para llevar a cabo procesos de captura y verificación de huellas.

Clasificación estándar de los scanners específicos: [TAPIADOR, 2005]

a) Tecnología óptica: Consta de un sensor de imagen de tipo CCD (Couple Charge Device) Dispositivo de acoplamiento de carga, elemento de captura de imagen, dispone de un juego de lentes, una matriz de fotosensores que convierte la radiación luminosa en una tensión proporcional, se muestra en la figura N.º 1.

b) Tecnología capacitiva: Usa un sensor electromagnético, el sistema detecta la diferencia de capacidades que existen entre la huella y el propio sensor. Es necesario observar que las características eléctricas más importantes de la piel humana son la impedancia y la capacidad siendo su modelo eléctrico equivalente a una matriz de resistores y capacitores en paralelo, como se muestra en la figura N.º 2.

   La función del sensor mide la capacidad existente entre él y la zona de la piel en contacto con la platina de crestas y la traduce a niveles de gris.

   Existen problemas como el sudor humano presenta una elevada constante dieléctrica. Esto produce la

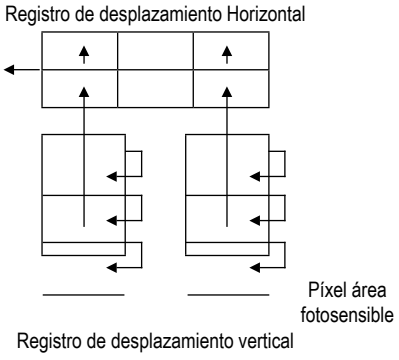

Figura N.º 1. Estructura reticular del CCD y sistema de vaciado de información.

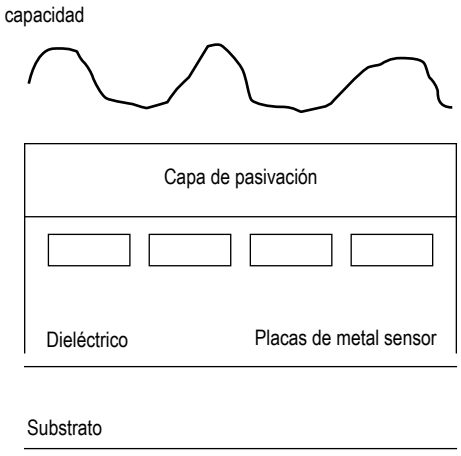

Figura 2. Esquema de la arquitectura.

saturación del sensor en una huella húmeda. En la captura de imagen de la huella ésta se representa por una imagen oscura, mientras la excesiva sequedad de la piel provocará una captura de huella casi tenue.

c) Tecnología ultrasónica: Este tipo de sistema envía un barrido de ondas ultrasónica que son mayores de 20KHz, que rebotan sobre la base de la huella. Es una tecnología de última generación para capturar huella dactilar, de alta resolución, el inconveniente es su elevado costo.

2.3.1.1 Software de soporte:

Los lectores integrados con un software de ayuda que operan como interfaz para realizar al adquisición de las huellas dactilares. La mayoría de dispositivos de captura de huellas van acompañados del software de gestión que permiten, entre otras tareas, el control de acceso al computador mediante la verificación de bloqueo del salva pantallas o la encriptación de datos. [TAPIADOR], 2005]

2.3.1.2 Reconocimiento de huellas dactilares:

Las técnicas de reconocimiento de huellas se dividen en dos categorías: [LIN, 1998].

A. Técnicas locales o analíticas: basadas en minucias, la dificultad que presenta es la extracción de minucias en imágenes de baja calidad.

B. Técnicas globales: basadas en la correlación, su ventaja con respecto a la técnica anterior es que necesita algoritmos de alineación de alta precisión y sensibles a las traslaciones y rotaciones de la huella.

Se utilizan más las técnicas locales dado que estas son más generalizadas en su uso.

Los pasos del proceso de identificación de una persona a partir de su huella dactilar:

1. Captura de huella: Este proceso depende del dispositivo de captura y puede almacenar la imagen de una de varias huellas dactilares para su posterior análisis.
2. Creación del modelo: Se extraen las minucias o puntos característicos de la huella presentes en la imagen adquirida y se almacenan en un archivo llamado patrón de la huella, muy necesario para la posterior comparación con la huella a reconocer.
3. Comparación del modelo: En este proceso se realiza la tarea de verificación / identificación de huellas dactilares. Verificación: Comparar el patrón de referencia con la huella candidata, una vez parametrizada, después de extraer las minucias presentes en la misma. Identificación: Comparar la huella candidata parametrizada con los patrones almacenados en la base de datos del sistema de identificación.
4. Verificación e identificación: La verificación se lleva acabo a partir del número obtenido en el proceso anterior (0 y 1, que se refiere al nivel de semejanza entre el modelo de referencia y modelo candidato).

El número de semejanza se compara con el umbral de seguridad establecido por el sistema. Del resultado de comparar se obtendrá la verificación o no del individuo candidato. La Identificación entrega como el resultado a la persona que presenta un patrón con mayor nivel de similitud con respecto a la entrada biométrica parametrizada.

En la etapa de reconocimiento de huellas dactilares existen dos algoritmos como son:

a) Algoritmo de alineamiento: Realiza cálculos mediante parámetros de rotación y traslación que conduzca al mayor nivel de correspondencia espacial al ajustar la huella parametrizada con el patrón. Los pasos del algoritmo son:

1. Seleccionar un par de minucias de referencia (una de cada imagen).
2. Determinar el número de pares de minucias que se corresponden.

3. Repetir el proceso de selección para cada uno de los pares de combinaciones posibles de minucias de referencia que presentan características locales comunes.
4. El par de minucias de referencia final seleccionado es contabilizado un mayor número de pares de minucias que se corresponden y en consecuencia el que ha estimado el mejor alineamiento.
5. Calcular los parámetros de rotación y traslación.
6. Aplicar parámetros de rotación / traslación calculado a todas las minucias del modelo de prueba.

b) Algoritmo de comparación de modelos: Cada vez que una huella acceda al sistema extrae su patrón biométrico de minucias y compara con cada patrón almacenado en la base de datos. El algoritmo de comparación entre modelos de entrenamiento y prueba consta de 2 partes:

1° parte: Ordena las minucias de los dos modelos para formar dos cadenas de puntos en coordenadas polares, el uso de las coordenadas se debe a que las deformaciones no lineales que aparecen en las huellas presentan siempre una zona no consistente, perdiéndose estas características a medida que los puntos se alejan de esta zona en direcciones radiales, el punto de máxima consistencia es la minucia de referencia que se tomará como centro de coordenadas polares del sistema. Las dos cadenas se constituirán en dos patrones a tratar por el algoritmo de comparación.

2° parte: Compara los dos vectores a partir de la distancia euclidiana entre minucias, dando resultado la identificación que corresponde al patrón. [REJMAN, 2002]

2.4. Estándares Biométricos:

Estándar es un conjunto de reglas que deben cumplir los productos, procedimientos o investigaciones que afirmen ser compatibles con el mismo. Los estándares ofrecen ciertos beneficios como reducción de diferencias entre productos, generando estabilidad, madurez y calidad en beneficio de los consumidores. La carencia de estándares biométricos a nivel industrial ha dificultado el desarrollo de aplicaciones.

2.4.1 El papel de los estándares biométricos:

Actualmente la mayoría de aplicaciones de tecnología biométrica usan tecnología propietaria (no estándar) de las empresas que las fabrican. [NANAVATY, 2004].

Los dispositivos biométricos estándares varían en la forma de comunicarse así como las aplicaciones, métodos que se utilizan para extraer las características con información discriminante de las muestras biométricas como huellas dactilares, voz, imagen y otras que se captan y procesan con sus propias técnicas y métodos de comparar patrones.

2.4.2 Interfaces de Programación de Aplicaciones:

Los objetivos de la industria biométrica es que tanto desarrolladores e integradores de aplicaciones que usen la tecnología biométrica a fin de que el trabajo sea un proceso fácil, bien documentado, por otra parte reducir los costos. El desarrollo de una Interfaz de Programación de Aplicaciones (API) estándar asegurará a los desarrolladores el uso de tecnologías y productos biométricos desde una perspectiva o enfoque común. (1DW y 2DW), se presenta la Tabla N.º 1 de Estándares:

3. SEGURIDAD

La tecnología de la seguridad es un campo muy actual, incluso se le denomina industria de la seguridad. La seguridad informática en particular se hace necesaria por cuanto la información y los datos corporativos crecen y cada vez es más difícil protegerlos, dado que la información se encuentra no solo en dispositivos estáticos (servidores, computadores, estaciones de trabajo) sino en dispositivos móviles (USB de memoria flash, celulares) que pueden almacenar información corporativa muy valiosa.

La seguridad es un concepto que se basa en “seguridad holística” o “seguridad colaborativa”, lo ideal es que todos los departamentos dentro de la empresa trabajen conjuntamente para asegurar la infraestructura y los activos de la empresa, para ello son necesarias las políticas de gestión de seguridad. [MALLERY, 2005]. Las políticas de gestión de seguridad considera:

1) Reconocer a los empleados socios como “clientes” es decir que la gestión de seguridad para los profesionales en informática deben identificar a los empleados socios como clientes, y a su vez este departamento esta diseñado para reconocer y apoyar

Estándar	Descripción
BioAPI (1998)	Estandariza la comunicación entre aplicaciones y dispositivos biométricos y almacenamiento de datos.
BAPI (2000)	Desarrollado por Microsoft, facilita el desarrollo de aplicaciones que usan parámetros biométricos en su SO.
ANSI X9.84 (2001)	Estandariza aspectos de seguridad relevantes para la industria: transmisión, almacenamiento, integridad y dispositivos biométricos.
ANSI NCITS (B10)	Estandariza el uso de tarjeta inteligente con información biométrica (huella digital, identificación).
HA-API (1997)	Estandariza la integración de sistemas de autenticación biométrica en aplicaciones comerciales que funcionan en red.
NBCT (1997)	Estandariza la evaluación de los sistemas y la tecnología biométrica. Plantea metodologías para la evaluación de dispositivos y su comparación
INCITS MI (2001)	Retorna los esfuerzos BioAPI Y CBEFF al fin de que fabricantes de USA de sistemas biométricos utilicen estándares comunes: Integración, almacenamiento, evaluación, transmisión de datos biométricos.

Tabla N.º 1. Estándares Biométricos.

las necesidades tecnológicas de la empresa para que se ejecuten sin problema y con eficacia.

Las políticas de gestión de seguridad en seguridad informática abarcan: Protección de datos, acceso local y remoto autorizado, costos, interrupción del sistema si es planificado ver momentos adecuados y reconfigurarlo, contar con el personal suficiente para el manejo del sistema, prevención de bloqueos de puertos concretos, prueba de los últimos cambios de configuración esto para entornos de producción, recuperar restaurar datos, en forma oportuna tras la pérdida o destrucción de datos, tener respaldos o backups.

2) Identificar a los responsables claves de la gestión de seguridad: De los datos y de la infraestructura o instalaciones a fin de mantener una postura fuerte dentro de la seguridad

Los departamentos de la empresa juegan un papel significativo en el proceso de seguridad son: los recursos humanos, legal, seguridad física, seguridad informática, gestión y usuarios finales. Los productos y las tecnologías proporcionan una base sólida para las iniciativas de seguridad. Los productos por sí solo no son suficientes. La seguridad es un proceso, no es un producto. Tanto los procesos como las políticas requieren definirse por directivas, normas, reglas y deben ser aprobadas para poder ser implementadas dentro de la empresa. Una política de seguridad es un documento que representa la filosofía de la empresa, es una guía para los que conforman la empresa. Del estudio de seguridad visto, se selecciona para el modelo la seguridad relacionado al acceso a la instalación o infraestructura de la empresa.

4. PROPUESTA DE TECNOLOGÍA BIOMÉTRICA

El estudio de "Tecnologías Biométricas Aplicado a la Seguridad en Organizaciones", luego del estudio de diversas tecnologías biométricas y de seguridad se propone la tecnología biométrica estática, mediante huella dactilar con los sistemas: Automatic Fingerprint Authentication System (AFAS) ¿Es quién dice ser? y Automatic Fingerprint Identification System (AFIS) ¿Quién es?, su desarrollo mediante software libre.

La identificación y verificación de una persona (administrativo y / o docente) en el modelo propuesto de control de asistencia del personal administrativo y docente de la Facultad de Ingeniería de Sistemas e Informática.

El modelo propuesto del sistema biométrico de huella dactilar utiliza el siguiente algoritmo:

Input: Identidad y la imagen de la huella

Output: La respuesta puede ser SÍ o NO.

Automatic Fingerprint Identification System (AFIS) ¿Quién es? Para lo cual se tiene:

Input: Solo la imagen de la huella

Output: Lista de identidades con puntuación respectiva.

El diseño del modelo propuesto para el sistema biométrico consta de:

Input: personal administrativo docente de la FISI es identificado por el Sistema de Control de Asistencia de la FISI-UNMSM, que ingresa al Sistema Automatice Fingerprint Autenticación System (AFAS).

Output: puede ser un ID: SI es igual al del patrón del sistema de control de personal de la FISI o NO, no encuentra en el patrón del sistema, finaliza en ambos casos con la emisión de reportes.

En este Sistema se consideran las fases de Identificación y Verificación:

Toma de huella: Proceso de segmentación mediante binarización y esquelitización.

Identificación (ID): Clasificación y coincidencia es un proceso de extracción de minucias a través de patrones almacenados en la base de datos del Sistema de Control de Personal, se accede para realizar consultas (querys), si existen coincidencias (matching), la respuesta es SÍ, se continúa el proceso con otros usuarios, sino la respuesta es NO, repetir el proceso o en su defecto la base datos no almacena el de ese usuario, como se muestra en el esquema general del diseño del sistema biométrico de la figura N.º 3.

El proceso de implantación para el sistema biométrico del modelo propuesto consta de las siguientes:

Interfaz de inicio de sesión que accesa el personal administrativo o docente de la FISI como:

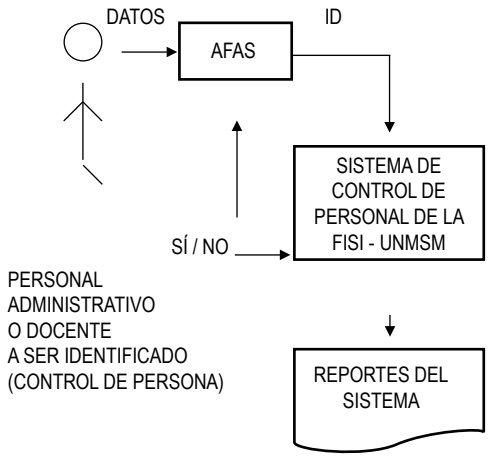

Figura N.º 3. Esquema general del sistema biométrico

Input: El personal administrativo o docente inscribe su huella dactilar e ingresa su código.

Output: el sistema presenta de inmediato su fotografía, SÍ el personal administrativo/docente está identificado y presiona Validar. Si no le presenta patrones de huellas dactilares y repite el proceso.

5. ANÁLISIS Y DISCUSIÓN

El presente estudio es básico, adaptativo y aplicativo, pertenece a las áreas de biometría y seguridad, y se ha profundizado sobre tecnologías biométricas y de seguridad, y aplicaciones. La técnica biométrica en aspectos de seguridad y control aún no está utilizada, debido a los costos elevados de software propietario y a los dispositivos de captura de datos. Lo más usado en nuestro medio en entidades privadas y públicas son tarjetas de crédito, tarjetas de código de barras, tarjetas de bandas magnéticas. Las organizaciones virtuales de la nueva economía requieren utilizar tecnologías de seguridad para reducir la brecha de vulnerabilidad, para ello se recomienda usar tecnologías biométricas. [ARENAS, 2005]

Se propone el modelo biométrico de control de asistencia de personal administrativo y docente de la Facultad de Ingeniería de Sistemas e Informática - UNMSM, me-

Las fases desarrollo del sistema biométrico del modelo propuesto:

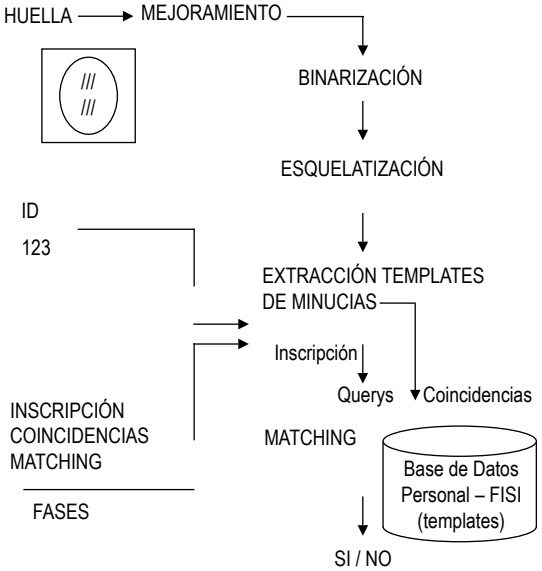

Figura N.º 4. Fases de desarrollo del sistema biométrico para el modelo propuesto.

diante la tecnología biométrica estática huella dactilar. Considerando que los dispositivos para captura y proceso con huellas dactilares no son muy costosos, y para su desarrollo utilizar software libre. Para implementar esta propuesta será necesario en la FISI- UNMSM, realizar una gestión de seguridad con políticas, directivas de seguridad y aprobación de la misma y del sistema biométrico por las instancias pertinentes de la Facultad y Universidad (desde la Oficina de Personal de la Facultad hasta el Consejo de Facultad de la Facultad) y en la Universidad.

6. CONCLUSIONES

1. El estudio constituye un aporte en el área de la tecnología biométrica y seguridad en las organizaciones
2. Las tecnologías biométricas facilitan la identificación de personas en las entidades
3. La industria biométrica en nuestro medio puede desarrollarse, usando software libre.
4. El uso de estándares biométricos facilitará el crecimiento de la industria biométrica.
5. El estudio propone un modelo de proceso de control de asistencia del personal administrativo y docente de la Facultad de Ingeniería de Sistemas e Informática - UNMSM, mediante biométrica estática (huella dactilar).

7. REFERENCIAS BIBLIOGRÁFICAS

[1] [ARENAS, 2005] ARENAS, A., "Trust and Security Virtuals Organization", Libro Resumen CLEI, Colombia.

[2] [CLARKE,1994] CLARKE, R., "Human Identification for Information Systems: Management Challenges and Public Policy Issues",. Info Technology, People, 1994.

[3] [JAIN, 1994] JAIN, A., Digital Image Processing. Springer-Verlag , 1997.

[4] [LIN, 1998] LIN, H., "Fingerprint Image enhancement: Algorithm and Performance Evaluation", IEEE.

[5] Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, N| 8, August 1998.

[6] [MALLERY, 2005] MALLERY, John, y otros, "Blindaje de redes", Editorial Anaya, Madrid, 2005.

[7] [NADLER, 1993] NADLER, M., Smith, E.P. Pattern Recognition Engineering. Editorial John Willey, 1993.

[8] [NANAVATY,2004] NANAVATY, S., "Biometric Identify, Verification in Networked world", Ed.John Wiley.2004.

[9] [PHILLPS, 2000] PHLLIPS, P, J., " An Introduction to Evaluation Biometric Systems", IEEE Computer, 2000.

[10] [REJMAN, 2002] REJMAN, M. Gerenne. "Secure Authentication using Biometric Methods", Management and Security Technical Report, Vol. 7, N° 3, 2002.

[11] [TAPIADOR,2005]TAPIADOR, M. "Tecnologías Biométricas Aplicadas a la Seguridad", Editorial, Rama. 2005.

[12] [WAYMAN, 1997] WAYMAN, James, L, "A Generalized Biometric Identification System Model", Proc. IEEE, Asilomar Conference on Signals, Systems, and Computers, 1997.

Direcciones web:

[1] DW Bio API: http://www.bioapi.org

[2] DW ANSI, American National Standards Institute: http://www.ansi.org

[3] DW ABIE, http://www.ii.uam.es-abie/