UNIVERSIDAD CENTRAL "MARTA ABREU" DE LAS VILLAS

VERITATE SOLA NOBIS IMPONETUR VIRILISTOGA. 1948

Facultad de Ingeniería Eléctrica

Departamento de Telecomunicaciones y Electrónica

Tesis presentada en opción al Título Académico de Máster en Telemática

MAESTRÍA EN TELEMÁTICA

Sistema biométrico para el control de asistencia de los empleados de la Empresa de Telecomunicaciones de Cuba

Autor: Ing. Jorge Francisco Caraballo Ríos

Tutor: Dr. C. Ramiro Pérez Vázquez

Santa Clara, Cuba

2016

"Año 58 de la Revolución"

Hago constar que el presente trabajo de Tesis fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la Maestría en Telemática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total, y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

Firma del Tutor

Firma del Jefe de Departamento donde se defiende el trabajo

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

"La sabiduría es el arte de entender que con el concurso de todas las fuerzas internas y externas nada es imposible"

DEDICATORIA

“A mi esposa por su paciencia, amor y apoyo incondicional”

“A mis amigos que han estado a mi lado en los momentos difíciles”

“A mis hijos, nietos y toda la familia”

“Para todos aquellos que me han ayudado a convertir un sueño en realidad”

AGRADECIMIENTOS

Un agradecimiento especial al colectivo de profesores de la Universidad Central “Marta Abreu” de las Villas por su profesionalidad y valor humano.

RESUMEN

La Empresa de Telecomunicaciones de Cuba tiene la necesidad de incrementar la confiabilidad del control de la asistencia de sus empleados, siendo este aspecto de gran importancia para incrementar la productividad del trabajo y el aprovechamiento de la jornada laboral. Los sistemas biométricos son una alternativa confiable para la autenticación de identidad, existiendo diversas técnicas para su desarrollo. Los sistemas biométricos basados en huella dactilar son un método efectivo, conveniente y seguro para la implementación del control de asistencia.

En el presente trabajo se propone el diseño y la evaluación de un sistema biométrico para el control de asistencia de los empleados de la Empresa de Telecomunicaciones de Cuba, tomando como base las experiencias y tecnologías utilizadas para tales efectos a nivel mundial. Se ha realizado un diseño conveniente y económico de todos los elementos que componen el sistema biométrico y, tanto el hardware como el software, dan respuesta a las necesidades planteadas, obteniéndose además múltiples reportes que permiten un control detallado de la asistencia de los empleados.

TABLA DE CONTENIDOS

Introducción

Los sistemas biométricos son una alternativa confiable y versátil para la autentificación de identidad, lo que permite su aplicación en distintas áreas como la seguridad, control de acceso y asistencia. La implementación de tecnologías en procesos administrativos de las instituciones es cada vez más necesaria, puesto que agiliza los trámites y facilita la toma de decisiones. En la actualidad, es cada vez más frecuente la necesidad de implementar sistemas que permitan de forma precisa la identificación y/o validación de personas para fines como la seguridad informática, control de acceso y control de asistencia, siendo la biometría el mejor método de identificación humana.

El control de asistencia tiene como objetivo poder determinar la ausencia o presencia de personal en un momento determinado y su importancia radica en el hecho de controlar la entrada y salida del mismo. Desde el punto de vista productivo y financiero, para una empresa, y específicamente para el caso de la Empresa de Telecomunicaciones de Cuba, los empleados son los principales protagonistas para el cumplimiento de los objetivos y las metas trazadas. Los métodos más usados en el control de asistencia en las empresas son la firma en libros, las boletas perforadas, las tarjetas de código de barras y las tarjetas de banda magnética. Estos métodos son muy vulnerables y fácilmente pueden ser falsificados por cualquier individuo.

Las técnicas biométricas se basan en los rasgos y características únicas e irrepetibles de los seres humanos, de forma tal que las mismas son viables para identificar positivamente a una persona, y de esta manera dejar obsoletos el uso de los métodos tradicionales que son vulnerables.

Los sistemas biométricos cuentan con características de universalidad, unicidad, estabilidad, facilidad de captura, aceptación por los usuarios, rendimiento, y son cuantificables; de igual forma con una gran variedad de métodos biométricos de identificación, siendo los más comunes los siguientes: sistemas de reconocimiento de voz, huella dactilar, rostro, iris, firma, exploración de la retina y contorno de la mano y el dedo.

Por tanto en este trabajo se plantea el siguiente problema científico: ¿Cómo incrementar la confiabilidad del control de asistencia del personal que labora en ETECSA?

El objeto de la investigación son los Sistemas Biométricos de Control de Asistencia y el campo de acción es el mecanismo de seguridad de control de asistencia basado en sistemas biométricos.

En consecuencia, el objetivo general de esta investigación es desarrollar un Sistema Biométrico de Control de Asistencia de los empleados de la Empresa de Telecomunicaciones de Cuba.

Para darle cumplimiento se declaran los objetivos específicos siguientes:

1. Caracterizar los sistemas biométricos de seguridad, haciendo énfasis en los utilizados para el control de asistencia.
2. Determinar el hardware y software a emplear en el sistema biométrico de control de asistencia.
3. Describir el funcionamiento y los reportes más utilizados en el sistema.
4. Evaluar los resultados del sistema propuesto.

De aquí que se propongan las tareas científicas siguientes:

- Descripción de las características generales de los Sistemas Biométricos de Seguridad.
- Descripción de las características específicas de los Sistemas Biométricos utilizados para el control de asistencia.

- Descripción de los equipos comerciales utilizados en los Sistemas de Control de Asistencia.
- Determinación del equipamiento a utilizar en el Sistema Biométrico de Control de Asistencia.
- Descripción de los software utilizados en los Sistemas de Control de Asistencia.
- Determinación del software a utilizar en el Sistema Biométrico de Control de Asistencia.
- Diseño de una aplicación para el control de asistencia y generación de reportes.
- Descripción del funcionamiento y diseño del Sistema Biométrico de Control de Asistencia propuesto.
- Evaluación de los Reportes de Incidencias más utilizados en el sistema.
- Evaluación de los resultados del sistema empleado.

Como aporte metodológico, el diseño e implementación de este Sistema Biométrico de Control de Asistencia utilizado en la Empresa de Telecomunicaciones de Cuba, puede ser extendido al resto de las entidades del país. El impacto social de este sistema está dado por un estricto control de la asistencia y permanencia de los empleados de la entidad, lo que redunda en un mayor rendimiento de la empresa en el cumplimiento de sus metas e indicadores. El impacto ambiental radica en el ahorro de los medios que se usaban anteriormente en el control de asistencia, tales como hojas, bolígrafos y tóner. El impacto económico de este sistema radica en un mayor rendimiento de la empresa, expresado en el incremento de los ingresos de la misma, aportado por una gestión eficiente de sus empleados.

Los métodos y técnicas utilizados fueron el método de análisis-síntesis, la medición y estadísticos matemáticos.

La estructura de la tesis consta de introducción, primer capítulo llamado “Sistemas Biométricos de Seguridad”, donde se caracterizan los Sistemas Biométricos de seguridad, profundizando en los sistemas empleados para el control de asistencia.

El segundo capítulo llamado “Diseño de un Sistema Biométrico de Control de Asistencia”; en él se realiza una descripción y evaluación de los equipos biométricos comerciales más utilizados en el Control de Asistencia, se establecen las relaciones entre calidad, precio y funcionalidad de los equipos biométricos para el control de asistencia, determinando el óptimo para ser utilizado, así como se caracterizan los software utilizados en estos sistemas, determinando el utilizado en el proyecto. Además, se presenta una aplicación personalizada en función de los requerimientos del sistema y se precisa la metodología para su instalación y puesta a punto.

En el tercer capítulo llamado “Funcionamiento y Evaluación de los resultados”, se aborda el funcionamiento del Sistema Biométrico, se describen los Reportes de Incidencias más utilizados y se evalúan los resultados.

Las conclusiones, recomendaciones, bibliografía y anexos le siguen a continuación.

El resultado esperado es realizar un diseño conveniente, económico y eficiente de un Sistema Biométrico para el control de asistencia en la Empresa de Telecomunicaciones de Cuba.

CAPÍTULO 1. Sistemas Biométricos de Seguridad

1.1. Introducción

Reviste gran importancia el uso de los sistemas biométricos de seguridad en el ámbito empresarial a nivel mundial. El interés en el empleo y la investigación de estos sistemas se incrementa día a día, dada las limitaciones existentes en los sistemas actuales de identificación de una persona. En la actualidad existen múltiples sistemas biométricos de seguridad, basados en el reconocimiento de huellas dactilares, cara, voz, iris, geometría de la mano, cada uno de ellos con sus ventajas y desventajas.

El concepto clásico de biometría denota la aplicación de técnicas matemáticas y estadísticas al análisis de datos en las ciencias biológicas. Dentro del contexto tecnológico, la biometría expresa la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características físicas o de comportamiento de las personas con el objetivo de establecer una identidad. Un sistema biométrico es todo aquel que realiza labores de biometría de manera automática. En otras palabras, se trata de sistemas basados en medir y analizar las características físicas y del comportamiento humano con propósito de autentificación.

Con el avance tecnológico, nuevos instrumentos aparecen para la obtención y verificación de huellas digitales, se comienzan a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo, el calor facial, la voz, la mano o la firma. Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser, posiblemente, el mejor método de identificación humana [1].

1.2. Definición de las características biométricas

Existen una serie de requisitos para que se pueda definir un sistema como sistema biométrico. Estos requisitos dependen de las características que se utilizan como parámetros de identificación y clasificación. Para poder decir que una característica es biométrica, ésta debería cumplir las siguientes condiciones [1]:

- Universalidad: si las características se pueden extraer de cualquier usuario o no.
- Unicidad: la probabilidad de que no existan dos sujetos con las mismas características.
- Estabilidad: si las características que se extraen permanecen inalterables en relación con diversos parámetros (tiempo, edad, enfermedades, etc.).
- Facilidad de captura: si existen mecanismos sencillos de captura de los datos biológicos o de comportamiento del sujeto.
- Rendimiento: o tasas de acierto y error.
- Aceptación por los usuarios
- Robustez frente a la burla del sistema: si la técnica puede reconocer el falseamiento de los datos capturados (uso de fotos, dedos de látex, etc.)
- Costo

1.3. Ventajas del uso de un sistema biométrico

Son claras las ventajas que se obtienen al utilizar sistemas biométricos. La utilización de sistemas biométricos libera al usuario del uso de elementos externos auxiliares. De forma resumida: el usuario no tiene nada que recordar, nada que cambiar y nada que perder. Proporciona un nivel más alto de seguridad ya que los parámetros utilizados son unívoca "firma" de una característica humana que no puede ser fácilmente adivinada o descifrada. La biométrica explota el hecho de que ciertas características biológicas son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto las hace más confiables, amigables y seguras que las contraseñas. En el pasado, el procesamiento

biométrico era hecho manualmente por gente que física y mentalmente comparaba huellas dactilares contra tarjetas, rostros contra fotos de pasaportes y voces contra cintas grabadas.

Hoy en día, dispositivos tales como escáneres, videocámaras y micrófonos pueden, electrónicamente, capturar y entregar estas mismas características biométricas para automatizar procesos y comparaciones. Cada tecnología biométrica (huella dactilar, rostro, voz, etc.) tiene sus propias características, variedades y certezas. Los niveles de precisión biométricos pueden variar pero son siempre más confiables que el 100% de falsas aceptaciones experimentadas con las contraseñas prestadas o robadas.

El problema de resolver la identidad de una persona se puede clasificar fundamentalmente en dos tipos distintos de planteamientos: reconocimiento (más popularmente conocido como identificación) y verificación. El reconocimiento se centra en determinar la identidad del sujeto dentro de un conjunto ya conocido de identidades. La verificación se encamina a confirmar o denegar la identidad aducida por una persona. En muchas situaciones de la vida cotidiana se requiere probar nuestra identidad, como por ejemplo cuando realizamos una compra con una tarjeta de crédito. Una verificación certera de la identidad de una persona podría disuadir la delincuencia y el fraude, dinamizar las transacciones comerciales y salvaguardar los recursos críticos [2].

1.4. Descripción de un sistema biométrico

Un sistema biométrico es básicamente un sistema reconocedor de patrones que opera del siguiente modo: captura un rasgo biométrico, extrae un conjunto de características y lo compara con otro conjunto de características almacenadas en una base de datos. Dependiendo de su finalidad, un sistema biométrico puede actuar de dos modos: verificación e identificación. Dentro del ámbito de los sistemas de reconocimiento, estos pueden tener dos finalidades: el reconocimiento positivo y el negativo. El reconocimiento positivo es aquel que busca comprobar que un usuario es realmente quien dice ser. En el caso de reconocimiento negativo, se trata de lograr determinar que un usuario es quien

afirma ser. En la Figura 1.1 se muestran las etapas de un sistema de Identificación Biométrica.

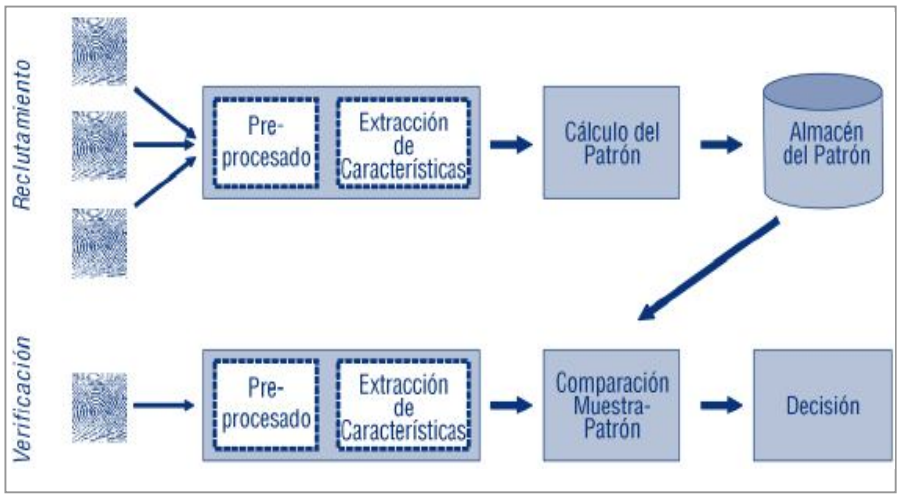


Figura 1.1: Etapas de un sistema de Identificación Biométrica.

A la hora de desarrollar un sistema de identificación biométrica, se mantiene un esquema totalmente independiente de la técnica empleada. Los sistemas, tal y como se puede ver en la Figura 1.1, se basan en dos fases totalmente diferenciadas [2]:

- Reclutamiento: en esta fase, se toma una serie de muestras del usuario, y se procesan, para posteriormente extraer un patrón, el cual se almacenará y será el conjunto de datos que caracterizará a ese usuario.
- Verificación: una vez que se tiene almacenado el patrón del usuario, éste puede utilizar el sistema con normalidad, y sus características son comparadas con el patrón almacenado, determinando el éxito o fracaso de esa comparación.

Cada fase se basa en una serie de bloques que hacen que las características biológicas o de comportamiento del individuo acaben siendo un elemento que lo identifique.

Estos bloques son:

- Captura: se toman los datos biofísicos o de comportamiento del sujeto. La toma de los datos depende, evidentemente, de la técnica biométrica empleada.

- Pre-procesado: en este bloque se adecuan los datos capturados para facilitar el tratamiento que tiene que realizar el siguiente bloque.
- Extracción de características: se puede considerar el bloque más significativo de la técnica a utilizar. Es el bloque en el que se fundamenta la capacidad del sistema de distinguir entre sujetos.
- Comparación: una vez extraídas las características de la muestra capturada, se han de comparar éstas con las previamente almacenadas, es decir, el patrón.

La identificación se puede realizar apoyándose en dos esquemas de funcionamiento del Sistema de Identificación Biométrica:

- Reconocimiento: También llamado identificación. Se basa en identificar a un usuario dentro de todos los usuarios que ya se encuentran en el sistema.
- Autenticación: También llamado verificación. En este esquema de funcionamiento, el usuario, al que se le toman sus características biométricas, también comunica su identidad. El sistema se encarga, entonces, de comparar las características extraídas, con el patrón del usuario indicado. Si la comparación supera un determinado umbral de parecido, se considera que el usuario es el indicado, rechazando la comparación en caso contrario. El patrón del usuario puede estar almacenado en una base de datos.

Tanto en verificación como en identificación, si la comparación es exitosa el sistema biométrico concede a la persona ciertos privilegios como, por ejemplo, acceso a un área restringida o acceso a su cuenta de banco. Cuando la comparación es fallida, los privilegios son negados [3].

1.5. Técnicas Biométricas de seguridad

Existe una gran variedad de tecnologías biométricas, tantas como características biométricas. Muchas de ellas se están aplicando en la vida real y otras están en proceso de estudio. Algunas características biométricas que se utilizan actualmente son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma de la mano, forma de la oreja, forma

de andar, forma de escribir en un teclado, firma, ADN y olor. Partiendo de estas características se han desarrollado dispositivos que han tenido mayor o menor éxito en el mercado. En la actualidad, los sistemas más usados son:

Sistemas de reconocimiento de voz

La voz es una característica que las personas utilizan comúnmente para identificar a los demás. Es posible detectar patrones en el espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares.

Tan solo basta recordar las veces en que se reconoce a alguien conocido por teléfono para comprender la riqueza de esta característica como método de reconocimiento. Los sistemas de verificación mediante la voz "escuchan" mucho más allá del modo de hablar y el tono de voz. Mediante el análisis de los sonidos que se emiten, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la garganta, también crean modelos de la anatomía de la tráquea, cuerdas vocales y cavidades. Muchos de estos sistemas operan independientemente del idioma o el acento de la persona. No obstante, la voz cambia por aspectos como la edad, enfermedades y estados de ánimo. Es una técnica con uno de los mayores potenciales comerciales: los servicios de atención telefónica personal, como la Banca Telefónica. Es una técnica que se lleva estudiando durante varias décadas, existiendo innumerables métodos para realizar, tanto la extracción de características, como la comparación. Algunos métodos son dependientes del texto pronunciado (es decir, todo o parte del texto que se recita debe ser idéntico en todas las ocasiones), mientras otros son independientes del mismo (pudiéndose recitar cualquier locución para realizar la identificación) [4].

Huella Dactilar

Las yemas de los dedos tienen una piel corrugada con líneas que forman una especie de surcos de un lado a otro del dedo.

El flujo de estos surcos no es continuo y está lleno de terminaciones y bifurcaciones (minucias) que forman un patrón, diferente en todas las personas, que es la base para el

reconocimiento de huellas. Además, no cambian con el tiempo. La persona pone su dedo en un lector de impresión digital, que identifica los puntos clave de la huella de ese individuo, ingresa la información y permite el cotejo posterior de los datos. En cuanto a la extracción de características, existen principalmente tres filosofías: la correlación de imágenes, la extracción y comparación de minucias (uniones y terminaciones de los surcos de la huella), y la extracción y comparación de los poros del dedo.

Por ejemplo, aunque puede utilizarse cualquier dedo de la mano, por una cuestión de dimensión y comodidad, los dedos más utilizados son el índice y el pulgar. Su funcionamiento se basa en tomar una imagen de la huella y por medio de algoritmos reducir dicha imagen a una representación matemática de la huella ("plantilla"). Esta plantilla patrón se acumula en la memoria interna del equipo (junto con un número de identificación o PIN si se trata de un verificador, a fin de tener asociada la huella al individuo). Luego, cada vez que la persona necesite identificarse, ya sea para registrar su horario de ingreso o regreso al trabajo o activar una puerta o barrera, debe digitar su PIN (en el caso que sea un verificador) y a continuación colocar su dedo (el mismo que registró originalmente) en el lector. Este proceso de escaneo de la huella digital puede apreciarse en la Figura 1.2 que se muestra a continuación [5].

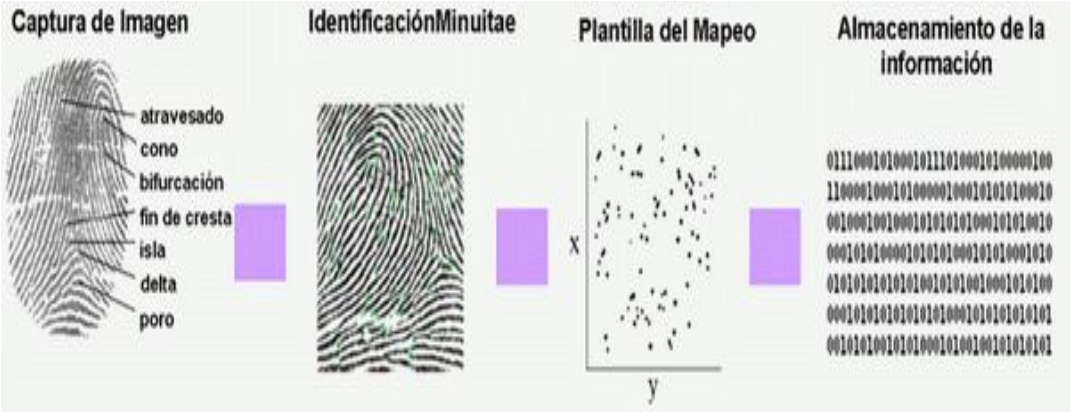


Figura 1.2: Proceso común de escaneo de la huella digital.

Rostro

En el reconocimiento facial los sistemas extraen los rasgos faciales de los usuarios para su identificación. La fuente para realizar la identificación puede ser tanto imágenes fotográficas como de vídeo. La identificación se puede hacer en 2D, 3D o una combinación de ambas. El objetivo de un sistema de reconocimiento facial es, generalmente, el siguiente: dada una imagen de una cara «desconocida», o imagen de test, encontrar una imagen de la misma cara en un conjunto de imágenes «conocidas», o imágenes de entrenamiento.

La gran dificultad añadida es la de conseguir que este proceso se pueda realizar en tiempo real. Tiene la desventaja de que las características de la cara varían por la edad, el maquillaje, el peinado, las gafas, la postura y las condiciones de luz, por lo cual en algunos casos no es útil para verificar la identidad. Los métodos para el reconocimiento del rostro utilizan principalmente estas cuatro técnicas: geometría facial, patrones de la piel, temperatura del rostro y sonrisa.

En la actualidad existen muchos grupos de investigación trabajando en esta técnica con diversos métodos (estudios morfológicos, transformadas multiresolución, etc.). Los resultados que se están consiguiendo son bastante prometedores, aunque le falta todavía bastante hasta llegar al nivel de otras técnicas [6].

Iris

El iris es la parte coloreada del ojo y está compuesto por un tejido fino que tiene la apariencia de líneas radiales y capas cuando se le examina de cerca. Esto crea un patrón único en cada persona que es el mismo durante toda la vida. Esta técnica fue impulsada por John G. Daugman en 1993. Los resultados obtenidos son, sin lugar a dudas, unos de los mejores de la actualidad, teniendo en cuenta que las características en las que está basada, el patrón de la textura del iris ocular, permanece inalterable durante la vida del sujeto debido a la protección que le proporciona la córnea. Por otro lado, los estudios sobre la unicidad de sus características, la han colocado muy por encima de la huella dactilar. Su gran inconveniente es el costo de los equipos, aunque teniendo en cuenta el grado de

fiabilidad alcanzado, existen numerosas aplicaciones de alta seguridad que podrían usar esta técnica.

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado, usando una cámara de alta resolución. Generalmente esto se hace mirando a través del lente de una cámara fija, la persona simplemente se coloca frente a la cámara y el sistema automáticamente localiza los ojos, los enfoca y captura la imagen del iris, ésta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos suficiente para los propósitos de autenticación.

El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no [7].

Firma

Utilizada desde antes que la huella dactilar, esta técnica siempre se ha visto entredicha por la posibilidad de falsificaciones, debido a que está basada en características del comportamiento. Las nuevas tecnologías facilitan realizar, no sólo el estudio de la firma ya realizada, sino también el estudio del acto de firmar, captando mediante un bolígrafo especial o una tableta gráfica, parámetros como velocidad, paradas, posición del bolígrafo, fuerzas, etc. en el mismo acto de firmar. Existen diversos prototipos y algunos productos comerciales, pero su éxito comercial ha resultado relativamente decepcionante. La firma es un método de verificación de identidad de uso común. Diariamente las personas utilizan su firma para validar cheques y documentos importantes. Como la firma es una habilidad adquirida, se le considera un rasgo de comportamiento. Además es muy complejo reproducir la habilidad humana de identificar si una firma es o no auténtica. En biometría,

el uso de la firma para verificación de identidad se hace de una manera diferente a la tradicional. Dependiendo del sistema, tanto la superficie donde se firma como el bolígrafo utilizado pueden contener varios sensores. Estos sensores miden características mucho más allá que simplemente la forma o apariencia de la firma: la presión que se aplica sobre la superficie, el ángulo al cual se sujeta el bolígrafo y hasta la velocidad y el ritmo de cómo la persona ejecuta su firma son características capturadas por el sistema [8].

Exploración de la Retina

Se demuestra que el patrón de los vasos sanguíneos de la retina presenta una mayor unicidad que el patrón del iris. Además, la casi imposible modificación de ese patrón, así como la facilidad para la detección de sujeto vivo, la hacen ser considerada la técnica más segura. Sin embargo, la forma de hacer la exploración, mediante láser, provoca un rechazo casi total por parte de los usuarios, estando sólo indicada para entornos de extrema seguridad, donde los usuarios son pocos y conscientes del grado de seguridad necesario. La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, tan distinto como una impresión digital y aparentemente más fácil de ser leído, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura. En los sistemas de autenticación basados en patrones retinales, el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter-ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso [9].

Geometría del Contorno de la Mano y/o del Dedo

Se trata de una técnica en la que se estudian diversos parámetros morfológicos de la mano (o el dedo) del usuario, tales como anchuras, alturas, etc. La técnica basada en geometría

del dedo se puede considerar como una simplificación de la basada en contorno de la mano. El gran atractivo de esta técnica, debido a su simplicidad, bajo costo y mínimo tamaño del patrón, la han convertido en la técnica con mayor éxito comercial en el último par de años.

El reconocimiento de la mano se puede hacer en dos y tres dimensiones. Los sistemas de dos dimensiones buscan en la palma de la mano patrones en las líneas, estos patrones son casi tan distintivos como las huellas digitales. El sistema toma entonces las características de la palma, los compara contra el modelo de referencia, y procede en consecuencia. Los lectores de tres dimensiones, sin embargo funcionan de forma distinta. Estos miden las dimensiones de la mano (largo de los dedos, altura de la mano, etc.). Aunque no es la más segura de las técnicas biométricas, el uso de la palma de la mano como medida de autenticación ha resultado ser una solución ideal para aplicaciones de seguridad media y donde la conveniencia es considerada una opción mucho más importante que la seguridad o la precisión [10].

Sistema de autentificación biométrica de las venas

Este sistema captura la distribución de las venas de la palma de la mano o de los dedos. Está siendo muy utilizado en la actualidad debido a su fácil implementación y gran aceptabilidad por parte de los usuarios, ya que muchos de ellos no requieren de contacto físico [11].

Olor

Técnica muy reciente, se basa en reconocer a una persona a través de su olor corporal. Las grandes incógnitas se encuentran en ver el rendimiento de este tipo de técnica frente a perfumes, colonias, olores ambientales, contactos con otras personas, etc. [12].

Oreja

Al utilizar la forma de la oreja o su temperatura, diferentes en cada individuo, es posible verificar la identidad de una persona. Desde un punto de vista forense, se demuestra que la oreja de un individuo posee muchas características propias del mismo.

Es una técnica de estudio muy reciente y su gran inconveniente es la necesidad de que el usuario descubra su oreja frente a una cámara, lo cual puede ser incómodo en el caso de personas con el pelo largo, o de determinados condicionantes sociales, de educación, religiosos, etc. [13].

Caminar

Es una técnica basada en características del comportamiento, por lo que es muy susceptible de ser falseada por imitaciones. Su estudio se encuentra en la actualidad en pleno desarrollo.

Dinámica de teclado

Se basa en reconocer a una persona por la forma en que escribe a máquina. Se mantiene la hipótesis de que el ritmo de teclado es característico de una persona, y prototipos existentes parecen reafirmar esa hipótesis. Sin embargo, además de ser una técnica basada en el comportamiento, y por tanto potencialmente emulable, tiene la limitación de no poder ser utilizada con usuarios que no tienen facilidad a la hora de escribir a máquina [14].

ADN

Sin lugar a dudas, la única técnica capaz de identificar unívocamente a una persona. Su potencia en el campo de la identificación choca con la dificultad en el desarrollo de sistemas automáticos de identificación en tiempo real y cómodo para el usuario. Los últimos intentos tratan de tomar la muestra mediante captación del sudor del sujeto. Sin embargo habría que estudiar la reacción de los usuarios frente a ese modo de captar la muestra [2].

1.6. El sistema biométrico genérico

Aunque estos dispositivos se basan en tecnologías muy diversas, mucho se puede hablar considerándolos genéricamente. El gráfico que se aprecia en la Figura 1.3 muestra un sistema biométrico genérico de identificación, dividido en cinco subsistemas: colección de datos, transmisión, proceso de señal, decisión y almacenamiento de datos [2].

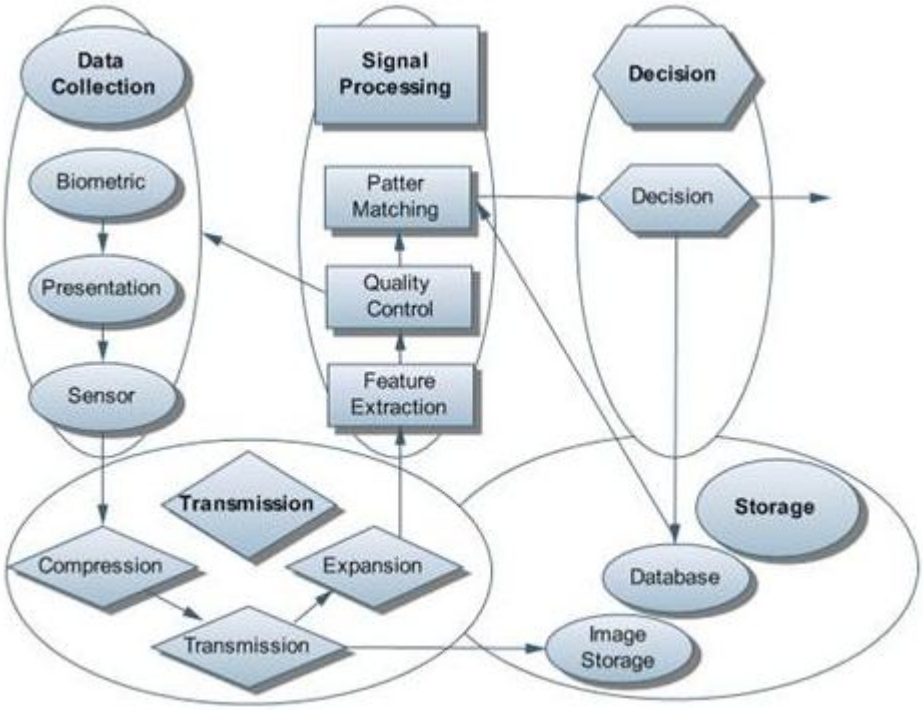


Figura 1.3: Sistema Biométrico genérico

1.6.1. Recolección de datos

Todo sistema biométrico, se inicia con la medida de algún rasgo de comportamiento o fisiológico de una persona. La importancia de todo sistema, es la hipótesis subyacente de que la característica biométrica medida es distintiva entre los usuarios y en un cierto plazo repetible para el mismo individuo. Con esto se quiere decir, es que las características deben variar considerablemente entre los individuos, pero no así para cada uno, en este caso, las variaciones deben ser muy pequeñas. Los problemas de medir y controlar estas variaciones, comienzan en el subsistema de la colección de datos. Las características del usuario deben ser presentadas a un sensor, la presentación de esa característica biométrica al sensor, introduce un componente de comportamiento, cuyos cambios afectarán la capacidad de repetición y distinción de la medida observada.

En los sistemas biométricos que se consideren abiertos, tanto la presentación de los rasgos al mismo, como el sensor que lleva a cabo la lectura, deberán ser estandarizados a los fines de asegurar que la característica biométrica recogida sea la misma que recogería cualquier otro sistema para el mismo individuo [15].

1.6.2. Transmisión

Algunos sistemas biométricos requieren de transmisión de datos ya que los recogen en un determinado lugar pero los almacenan y/o procesan en otro. En el caso de que la cantidad de datos sea elevada, la compresión de los mismos es fundamental a fin de utilizar poco ancho de banda para su transmisión y poco espacio para su almacenamiento, es por eso que se efectúa un proceso de compresión antes de que los mismos sean transmitidos y/o almacenados, y un proceso de descompresión para que sean legibles en su utilización. El punto negativo de la compresión/descompresión, es que generalmente causan pérdida en la calidad de la señal restablecida, es decir, la imagen pierde algo de calidad con respecto a la original. En un sistema abierto, los protocolos de compresión y de transmisión deben ser estandarizados, de manera que cada usuario de los datos pueda reconstruir (aunque con pérdida de calidad) la imagen original. Los estándares actualmente existentes son: huella digital, formato WSQ, imágenes faciales, formato JPEG, datos de voz, formato CELP [16].

1.6.3. Proceso de Señal

Una vez que la característica biométrica es adquirida y transmitida, se debe preparar para ser correspondida con otra. El primer paso es analizar el modelo biométrico verdadero de la presentación como así también las características del sensor, todo esto en presencia de las pérdidas por ruido y de señal impuestas por transmisión. El segundo paso es preservar el modelo biométrico a los fines de que esas cualidades sean distintivas y repetibles, desechando las que no lo sean o sean redundantes.

En algunos sistemas, la transmisión ocurre después de la extracción de la característica para reducir el requisito de mínimo ancho de banda y así minimizar la pérdida de calidad del original. Después de la extracción de la característica, o quizá antes o durante, se desea

controlar si la señal recibida del subsistema de colección de datos tiene la calidad requerida, a fin de solicitar si es necesario una nueva muestra del usuario. El funcionamiento de los sistemas biométricos, ha mejorado en los últimos años debido al desarrollo de este proceso de "control de calidad". La finalidad de este procedimiento de concordancia con el modelo, es comparar una muestra actual con la característica almacenada, a la que se llama modelo, enviando al subsistema de decisión la medida cuantitativa de la comparación.

Para la simplificación, se asumen modelos que requieran de "distancias pequeñas" al realizar la comparación con las muestras biométricas de la base de datos. Las distancias raramente, serán fijadas en cero, pues siempre habrá alguna diferencia relacionada con el sensor o relacionada con el proceso de transmisión o con el comportamiento propio del usuario [17].

1.6.4. Decisión

La política del sistema de decisión dirige la búsqueda en la base de datos, y determina los "matching" (concordancia) o los " no-matching" basándose en las medidas de la distancia recibidas de la unidad de proceso de señal. Este subsistema, en última instancia toma una decisión de "aceptación" o "rechazo" basada en la política establecida por el sistema.

Tal política podría ser declarar un "matching" para cualquier distancia más baja que un umbral fijo y "validar" a un usuario en base de este solo "matching", o la política podría ser declarar un "matching" para cualquier distancia más baja que un umbral dependiente del usuario, variante con el tiempo, o variable con las condiciones ambientales. Una política posible es considerar a todos los usuarios por igual y permitir sólo tres intentos con una distancia alta para el "matching" para luego volver una medida baja de la distancia. La política de decisión empleada es una decisión de la Gerencia, que es específica a los requisitos operacionales y de la seguridad del sistema. En general, bajar el número de no-matching falsos se puede negociar contra levantar el número de matching falsos. La política óptima del sistema depende de las características estadísticas de las distancias de comparación que vienen de la unidad de "matching "del modelo y de las penas relativas

para el matching falso y el no-matching falso dentro del sistema. En cualquier caso, en la prueba de dispositivos biométricos, es necesario evaluar el funcionamiento del subsistema de proceso de señal con independencia de las políticas puestas en ejecución mediante el subsistema de decisión [18].

1.6.5. Almacenamiento

Existen varias formas de almacenamientos a utilizar, esto depende del sistema biométrico en cuestión. Los modelos de las características obtenidas, son almacenados en una base de datos para su comparación en la unidad de ¨matching¨. En los sistemas que se basan en la correspondencia "uno a uno", la base de datos puede ser distribuida en tarjetas magnéticas por cada usuario, dependiendo de la política del sistema, no es necesaria ninguna base de datos centralizada, ya que generalmente la información almacenada no es voluminosa, se recuerda como ejemplo de esto, la necesidad de comparar la identidad de un empleado de una empresa, lo que para llevar a cabo este proceso, se busca la identidad sujeto en una base de datos de los empleados de toda la empresa, lo que implica una búsqueda reducida para determinar su pertenencia o no; aunque, en esta aplicación, una base de datos centralizada se puede utilizar para detectar tarjetas falsificadas o para reeditar tarjetas perdidas sin recordar el modelo biométrico. Los requisitos de velocidad del sistema dictan que la base de datos esté repartida en subconjuntos más pequeños, tales que cualquier muestra de la característica necesita solamente ser correspondida con la de los modelos salvados en una partición. Esta estrategia tiene el efecto de aumentar velocidad del sistema y de disminuir matching falsos a expensas de aumentar la tasa de no-matching falso. Esto significa que las tasas de error del sistema no son constantes con el aumento del tamaño de la base de datos y, además, esta relación no es lineal. Por lo tanto, las estrategias para particionar la base de datos representan una decisión bastante compleja. Si existe la posible necesidad de reconstruir los modelos biométricos a partir de los datos salvados, será necesario el almacenamiento de datos sin procesar. El modelo biométrico, en general, no es reconstituible a partir de los datos salvados. Además, los modelos se crean usando algoritmos propietarios de extracción de características, propios de cada fabricante. El

almacenamiento de informaciones en bruto permite cambios en el sistema o de equipamiento sin que sea necesario registrar nuevamente a todos los usuarios [19].

1.7. Sistemas biométricos basados en huellas dactilares

En la actualidad, los métodos más aceptados de identificación se basan en la colección de rastros dactilares y, últimamente, en las muestras de ácido desoxirribonucleico (ADN), cuyos grados de confiabilidad resultan casi infalibles. La mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación.

Estos sistemas, fundamentan su funcionamiento en el reconocimiento de las características de las huellas dactilares de los usuarios. Dependiendo del modo de operación en el que trabajen, se clasifican en:

Sistema Automático de Identificación por Huellas Dactilares (Automatic Fingerprint Identification System - **AFIS**)

Sistema Automático de Verificación por Huellas Dactilares (Automatic Fingerprint Authentication System - **AFAS**)

1.7.1. Reconocimiento de la huella digital

Los sistemas de reconocimiento de huellas digitales, tienen por tarea, el análisis y la comparación de los pliegues (crestas) y de minucias (lugar donde los pliegues del dedo, paran, bifurcan o se rompen). A efectos de evitar confusiones, se utilizan las palabras pliegues o crestas como sinónimos, ya que ellas se refieren a lo mismo. En la Figura 1.4 se puede observar un Sistema de reconocimiento de huella dactilar.

Figura 1.4: Sistema de reconocimiento de la huella digital

La huella dactilar, como se ha mencionado anteriormente, es un rasgo biométrico que ha sido utilizado desde hace siglos en la humanidad con la finalidad de poder identificar personas. Este rasgo es particular y único para cada individuo, teniendo origen durante la etapa fetal y permaneciendo inalterable a lo largo de toda la vida. Si bien el empleo de las huellas digitales data desde tiempos remotos, es en el siglo pasado donde han tenido un auge significativo gracias a la utilización y clasificación de las mismas por parte de las fuerzas policiales, quienes a través de los avances sobre esta porción del cuerpo humano, han logrado crear métodos efectivos para su utilización en la autenticación de personas. No Las huellas digitales son las primeras características biométricas que han sido utilizadas profesionalmente a nivel masivo y con una altísima tasa de aceptación a nivel mundial. Se puede definir a una huella dactilar o digital, como una representación morfológica de la superficie de la epidermis de un dedo. Posee un conjunto de crestas papilares, que generalmente aparecen dispuestas en forma paralela. De todas formas, estas líneas se interceptan y en algunos casos terminan en forma abrupta. Estos lugares, donde las crestas terminan o se bifurcan, se las conocen técnicamente con el nombre de minucias. Aproximadamente cada huella dactilar presenta entre 30 y 40 minucias, de las cuales solamente ocho pueden ser comunes entre dos personas. Algunas minucias de la huella dactilar se pueden apreciar en la Figura 1.5 que se muestra a continuación.

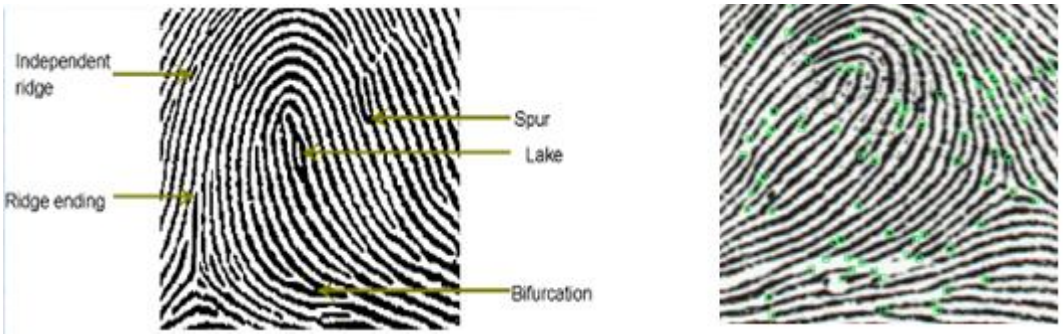


Figura 1.5: Algunas minucias de la huella dactilar- Cresta independiente (Independent ridge), Final de la cresta (Ridge ending), Ramal corto (Spur), Lago (Lake) y Bifurcación (Bifurcation).

Se estima que la probabilidad de que dos personas tengan las mismas huellas dactilares es aproximadamente de 1 en 64.000 millones [20].

Cada país determina independientemente, el número de minucias que utilizarán por huella, como ejemplo de esto, a continuación se mencionan algunos países con el número mínimo de minucias que establecen para su utilización en la verificación de personas:

- Israel 12
- Bulgaria 8
- Alemania 12
- Gran Bretaña 16
- Colombia 10

1.7.2. Clasificación de las huellas digitales

Cada huella digital tiene uno de cuatro modelos básicos:

- Arco
- Arco Entoldado
- Espiral
- Bucle

Los modelos básicos de la huella dactilar se pueden observar en la siguiente Figura 1.6. [20].

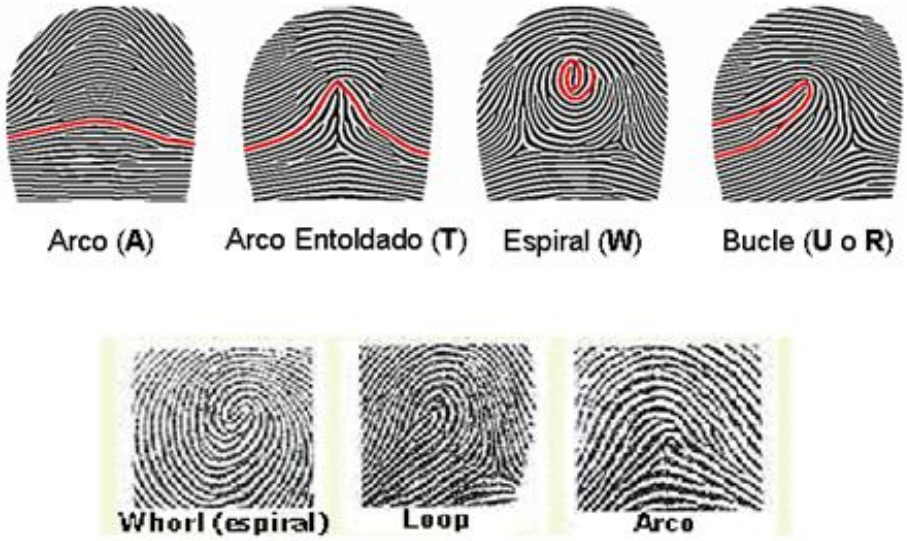


Figura 1.6: Modelos básicos de la huella

Los pliegues en el modelo de arco comienzan en una cara del dedo y en el extremo en la otra, formando una clase de arco concluido en el centro. Algunas huellas digitales combinan dos o más de estos modelos básicos. En un modelo del espiral (whorl), algunos pliegues forman los círculos más o menos concéntricos alrededor del centro del dedo. En el modelo del bucle, el comienzo de los pliegues es a partir de una cara del dedo, entonces alcanza la punta de la base (aproximadamente el centro) del dedo y del " bucle " de nuevo a la misma cara. Las impresiones digitales arriba expuestas, se distribuyen en la población de la siguiente manera:

- Espiral (whorl): 30%
- Bucle (loop): 65%
- Arco: 5%

Tan importante como el tipo de modelo son las minucias de una impresión, las puntas donde los pliegues paran, bifurcan, adaptan, o cambian de otras maneras [21].

1.7.3. Clasificación de los Pliegues

La clasificación de los pliegues se representa a continuación, estando bien detallados en la Figura 1.7 [21].

- **Ridge Ending (Final de Pliegue):** es donde un pliegue comienza o finaliza imprevistamente.

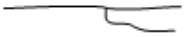
- **Ridge Bifurcation (Bifurcacion de Pliegue):** es el punto en donde un pliegue se divide en dos.

  - **Divergence:** es cuando dos pliegues corren en forma paralela y en un determinado lugar toman caminos opuestos.

  - **Lake:** es una bifurcación doble, una hacia la izquierda y otra hacia la derecha, formando un hoyo o lago.

- **Independent Ridge:** es un pliegue pequeño.

- **Spur:** es una combinación de dos pliegues independientes en una bifurcación.



- **Crossover:** es un pliegue independiente que atraviesa dos pliegues independientes.

Figura 1.7: Clasificación de los pliegues

Las minucias, además de ser clasificadas según su diseño, también se las identifica por su posición respecto a un sistema de coordenadas x y, la curvatura de los pliegues, el espacio entre los pliegues en esa punta, etc., cuestión que puede preciarse en la Figura 1.8. Como se puede deducir, la huella digital entera es el total de todas sus características, incluyendo el modelo y todas sus minucias.

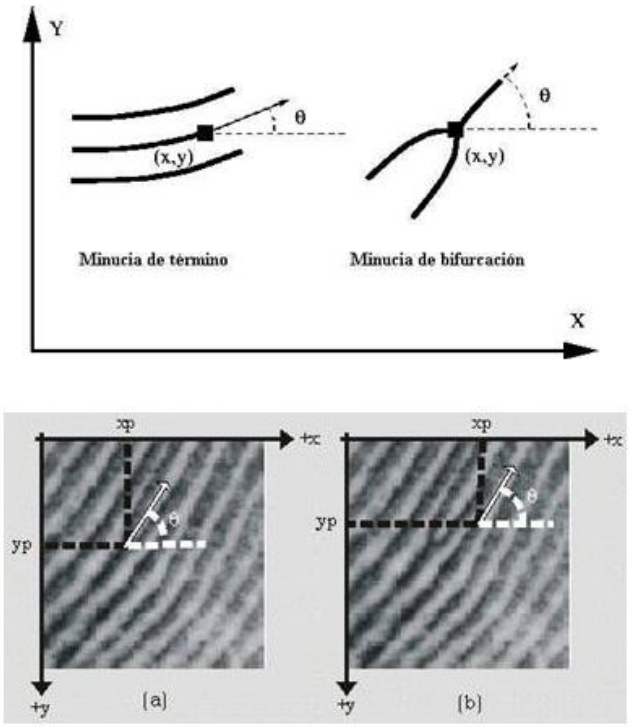


Figura 1.8: Minucias en términos de posición y dirección

Las minucias y sus posiciones relativas son extraídas y utilizadas para la clasificación de las huellas dactilares, como se observa en la Figura 1.9.

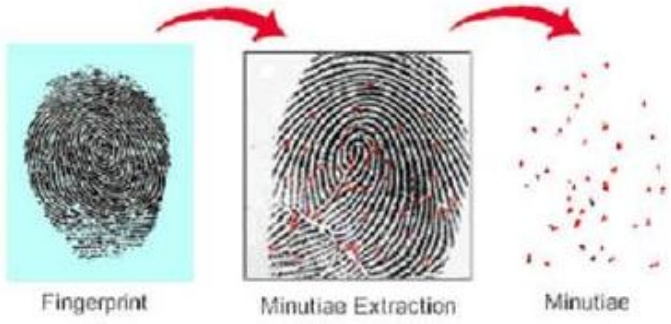


Figura 1.9: Extracción de las minucias

1.7.4. Técnicas de Adquisición de huellas

Existen dos modos diferentes de obtener huellas digitales, la primera se llama off-line, y es aquella en la cual se utiliza sustancias químicas, como por ejemplo las huellas obtenidas en papel luego de haber entintado el dedo del sujeto. El otro modo, es el llamado on-line, aquí la obtención de la huella dactilar se obtiene mediante un sensor biométrico, esta técnica también se la conoce con el nombre de live-scan [22]. Ambos modos se describen de la siguiente forma:

Modo Off-line

Estas técnicas usualmente funcionan de la siguiente manera: se aplica una sustancia sobre el dedo, luego la yema es apoyada sobre una superficie que reacciona con la sustancia, logrando que aparezca en ésta la impresión dactilar. La técnica más conocida y utilizada en unidades forenses y policiales emplea la tinta como la sustancia aplicada y el papel como la superficie, con la peculiaridad que el dedo debe ser rolado o rodado de un lado a otro de tal manera que la impresión dactilar resultante no presente borrones o manchas. En la práctica, esta técnica no es la más adecuada, puesto que un exceso de tinta puede manchar una parte o la impresión completa, mientras que una deficiencia de tinta producirá una impresión borrosa, afectando en gran medida su calidad y por consiguiente generando errores en el proceso de comparación.

Otras técnicas utilizan sustancias que no manchan la piel y originan una reacción sobre la superficie en la que el dedo es apoyado. Un caso especial utilizado en aplicaciones forenses es la obtención de impresiones dactilares latentes sobre los objetos, como las que se dejan al sujetar una copa de cristal. La captura se realiza mediante polvos químicos que se adhieren a la impresión dactilar latente, siendo ésta recuperada mediante una película adhesiva o a través de una iluminación especial y fotografía. Esta técnica de adquisición puede ser apreciada en la Figura 1.10 que se muestra a continuación [23].

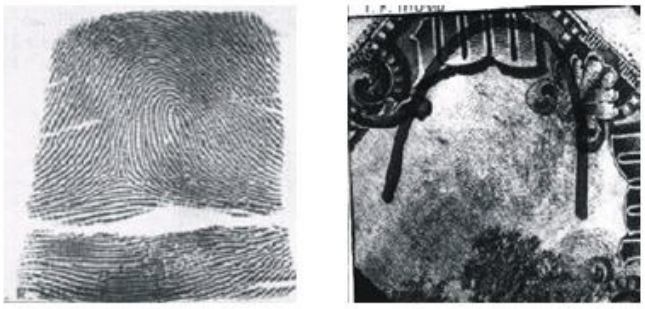


Figura 1.10: Impresión digital rodada y latente

Modo On-line

Las huellas on-line, se obtienen mediante la adquisición directa de la huella dactilar al colocar el dedo sobre la superficie sensible del sensor electrónico. El procedimiento de conversión de la huella capturada en una imagen digital depende de los principios físicos de funcionamiento del sensor utilizado. Ateniendo a estos principios físicos, puede establecerse la siguiente clasificación de sensores:

- **Sensores ópticos**

Entre estos sensores están aquellos que se basan en la reflexión de la luz sobre la yema del dedo (FTIR, Frustrated Total Internal Reflexion), los sensores basados en fibra óptica, los electro-ópticos y los sensores sin contacto.

- **Sensores de estado sólido**

A este grupo pertenecen los sensores capacitivos, térmicos, de campo eléctrico y piezo-eléctricos.

- **Sensores ultrasónicos**

Estos sensores utilizan ultrasonidos para obtener los pliegues dactilares

Los objetivos comunes a todas las técnicas de adquisición son: la reducción del costo económico del dispositivo; la reducción del tamaño del sensor; la mejora de la calidad de

imagen; el aumento de la resolución; y la reducción de la distorsión generada por el propio procedimiento de captura.

Por ejemplo, los dispositivos de estado sólido permiten cierta funcionalidad que no proporcionan los dispositivos ópticos: el control automático de ganancia y el control del sensor por programa. La ganancia en la mayoría de los captadores ópticos sólo puede variarse manualmente para cambiar la calidad de la imagen. Los dispositivos de estado sólido permiten modificar la sensibilidad de determinadas zonas del sensor para controlar la calidad. Pueden combinar el control automático de ganancia con la realimentación para conseguir altas calidades de imagen. Por ejemplo, en estos dispositivos es frecuente el bajo contraste de la imagen originada cuando la piel del dedo está muy seca. Como consecuencia, puede aumentarse la sensibilidad, para que en una segunda adquisición, se mejore la calidad. También puede aumentarse localmente la sensibilidad de determinados píxeles del sensor, cuando se detecta que la presión ejercida en determinadas zonas de su superficie origina un bajo contraste en la imagen [24].

Los lectores de huella digital típicamente empalman varias imágenes de huellas digitales para encontrar una que corresponda. En realidad, este no es un modo práctico para comparar las huellas digitales. Una imagen borrosa puede hacer que dos imágenes de la misma huella se vean bastante diferentes, así que raramente se podrá obtener un empalme perfecto. Adicionalmente, utilizar la imagen completa de la huella digital en un análisis comparativo utiliza muchos recursos del procesador, y además hace más sencillo robar los datos impresos de la huella de alguien.

En vez de esto, la mayoría de los lectores compara rasgos específicos de la huella digital, las minucias anteriormente mencionadas. Típicamente, los investigadores humanos y computadoras se concentran en puntos donde las líneas de las crestas terminan o donde se separan en dos (bifurcaciones).

El software del sistema del lector biométrico utiliza algoritmos altamente complejos para reconocer y analizar estas minucias. La idea básica es medir las posiciones relativas de las

minucias. Una manera simple de pensar en esto es considerar las figuras que varias minucias forman cuando dibujas líneas rectas entre ellas. Si dos imágenes tienen tres terminaciones de crestas y dos bifurcaciones formando la misma figura dentro de la misma dimensión, hay una gran probabilidad de que sean de la misma persona. En la Figura 1.11 se observa gráficamente como es obtenida la plantilla de huella a partir de la extracción de las minucias.

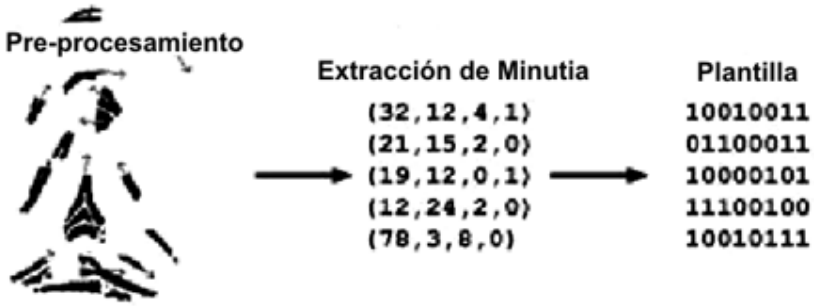


Figura 1.11: Obtención de la plantilla de la huella

Para obtener una coincidencia, el sistema del lector biométrico no necesita encontrar el patrón entero de minucias en la muestra y en la imagen almacenada, simplemente debe encontrar un número suficiente de patrones de minucias que ambas imágenes tengan en común. El número exacto varía de acuerdo a la programación del lector [25].

1.8. Tasa de falsa aceptación y falso rechazo

La Tasa de Falsa Aceptación (FAR, por las siglas en inglés de False Aceptation Rate) es el porcentaje de los usuarios que no están autorizados por el sistema pero que igual se les da acceso al mismo. La Tasa de Falso Rechazo (FRR, por las siglas en inglés de False Reject Rate) es el porcentaje de los usuarios autorizados por el sistema pero que se les niega el acceso. Si bien estas tasas de exactitud son útiles, y los fabricantes de sistemas biométricos las citan a menudo en sus descripciones del producto, algunos de estos valores no son reales y muchas veces son adulterados a efectos de poder sorprender al potencial cliente. Con respecto a estos valores, algunos fabricantes están destacando que sus productos tienen

una Tasa de Falsa Aceptación que varían entre 0.0001% y 0.1%, aquí se puede citar como ejemplo que en los Estados Unidos, los lectores biométricos de mano que están en la entrada principal de las centrales nucleares, tienen comprobadamente una Tasa de Falsa Aceptación del 0.1%. Con respecto a las Tasas de Falso Rechazo, se manejan valores entre 0.00066% y el 1.0%.

Es un hecho inevitable que los rasgos físicos de las personas varíen en un cierto plazo, especialmente con las alteraciones debido al envejecimiento o accidentes. Además de esto, se pueden citar otros problemas, como por ejemplo la humedad del aire, suciedad, sudor en las partes a ser analizadas, falta de entrenamiento en la utilización de los dispositivos biométricos por parte de los usuarios. Estas y otras consideraciones son las que limitan la exactitud de los dispositivos biométricos, pero de todas formas, son mucho más exactos que otras medidas o mecanismos de seguridad, ya que se basan en los rasgos del usuario y no en lo que tienen o en lo que saben.

Además de estos factores que se nombran, hay algunos otros que también son evaluados a la hora de determinar la calidad de un dispositivo biométrico, por ejemplo, existe lo que se llama la vulnerabilidad al fraude o barrera para atacar, en este caso, se prueba al sistema con una persona que quiere hacer un uso engañoso del mismo y el cual tratará de burlarlo de múltiples maneras a los fines de lograr su propósito, es decir, utilizar el dispositivo o sistema a pesar de no estar autorizado [26].

En este caso, el sistema biométrico deberá contar con características de seguridad que puedan reconocer a una persona viva, ya que es posible crear dedos de látex o silicona, grabaciones digitales de voz, prótesis de ojos, etc. que pueden llegar a burlar o pasar cualquier medida de seguridad biométrica, siempre y cuando estas no estén tecnológicamente aptas. A manera de ejemplificar las medidas de seguridad, se pueden citar un sistema infrarrojo para chequear las venas de la mano que detecta flujos de sangre caliente, lectores de ultrasonido para huellas dactilares que revisan estructuras subcutáneas de los dedos, lectores de iris que perciben los micro movimientos de los ojos de la persona

viva, etc., estas características eliminan cualquier posibilidad de éxito que puedan tener los métodos fraudulentos que utilizan plantillas, moldes, postizos, etc.

Otros de los puntos a tener en cuenta a la hora de evaluar la calidad de un dispositivo biométrico, son la exactitud, rapidez y robustez alcanzada en la identificación, como así también los recursos invertidos, cantidad de espacio en disco rígido para la instalación de la aplicación, efectos ambientales y/u operacionales, etc.

La aceptabilidad y estabilidad son dos rasgos muy importantes que también deberá contar un buen sistema biométrico.

La aceptabilidad, representa el grado en que las personas estarán dispuestas a utilizar un dispositivo biométrico, es muy importante recalcar que el sistema no debe intimidar ni representar peligro alguno para los usuarios, también deben inspirar confianza en su utilización. Por ejemplo, el reconocimiento del iris y/o retina puede intimidar a los usuarios, ya que los mismos deberán exponer su vista a un haz de luz para su escaneo, pudiendo producir desconfianza con respecto a que consecuencias a corto o largo plazo puede llegar a provocar el haz de luz enfocado directamente sobre el ojo.

Cuando se habla de estabilidad, se refiere por ejemplo si un sistema es útil para usuarios que son muy infrecuentes en su utilización, ya que como se plantea anteriormente, los rasgos biométricos cambian con el tiempo, pudiendo con esto provocar un falso rechazo por parte del sistema.

Una FRR puede provocar cierto descontento entre los usuarios del sistema debido al alto número de rechazos, en cambio una FAR elevada suscita un grave problema de seguridad, ya que permitiría el acceso a recursos por parte de personal no autorizado.

Si se quiere evaluar las prestaciones de un sistema biométrico, se utiliza lo que se llama Tasa de Éxito (Success Rate, SR), valor que se obtiene en base a una combinación de los dos factores anteriormente nombrados:

$SR = 1 - (FAR + FRR)$

La FAR y la FRR varían en función de las condiciones que se fijen para la identificación biométrica. Por ejemplo, en caso de utilizar el programa en entornos de máxima seguridad, se intenta que la FAR sea lo más pequeña posible, aunque esto implique un aumento significativo de la FRR. Para evitar un defasaje en la valorización de cualquiera de estos parámetros, es necesario fijar un umbral que permita igualar los dos factores, lo que permitirá obtener un óptimo funcionamiento del sistema. Este umbral se denomina Tasa de Error Igual (Equal Error Rate, EER), y es el que determinará, finalmente, la capacidad de identificación del sistema, esto significa que mientras más bajo sea el valor de EER, más exacto es el sistema. En la Figura 1.12 se muestra la correspondencia de dicha relación [27].

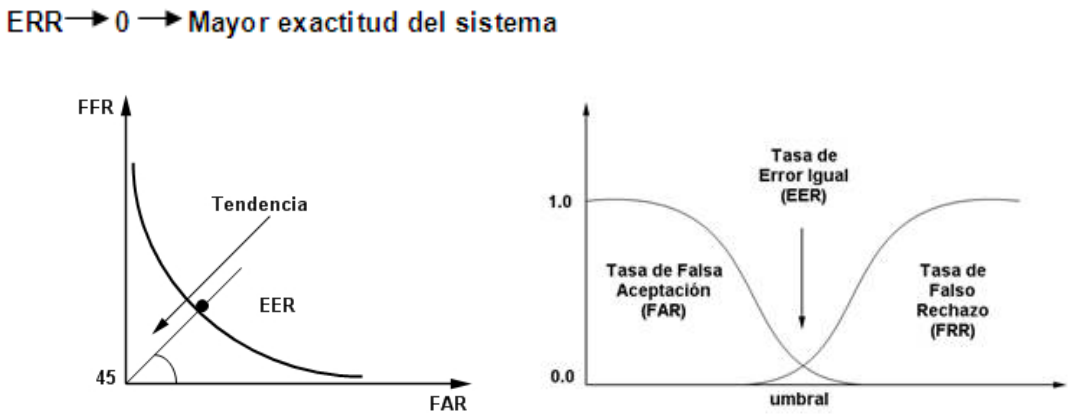


Figura 1.12: Correspondencias FFR y FAR

El punto de equilibrio se da donde FAR=FRR es decir, el punto EER. La FAR y la FRR son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco

requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa. El grado de seguridad deseado se define mediante el umbral de aceptación **u**, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo. En la Figura 1.13 se muestra una gráfica típica de la Tasa de Falso Rechazo y la de Falsa Aceptación como funciones del umbral de aceptación **u**para un sistema biométrico.

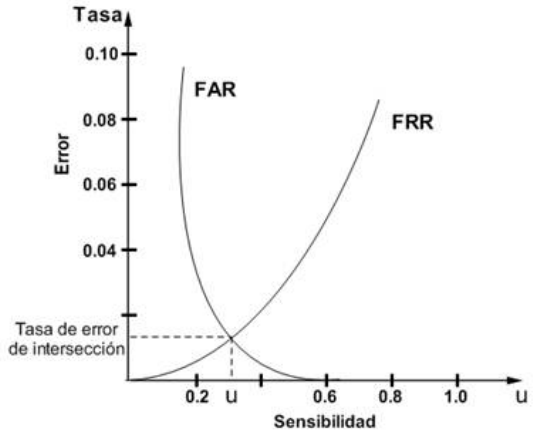


Figura 1.13: FRR y FAR como funciones del umbral de aceptación

Muy relacionado con los parámetros FRR y FAR, y sobre la base también de definir la exactitud de un sistema biométrico, se abordan los errores producidos en los sistemas biométricos (Ver Anexo 1) [28].

1.9. Marco regulatorio

Los estándares biométricos especifican las condiciones necesarias para que las tecnologías biométricas puedan ser eficaces e interoperables, y describen métodos para su integración con los sistemas de identificación y autenticación, y para el intercambio de información entre sistemas. La estandarización en el área de la biometría se está acelerando. Este

proceso está impulsado por el sector privado, por organizaciones de estándares internacionales así como por agencias gubernamentales de políticas y estándares.

Las principales son:

- ANSI/INCITS. American National Standards Institute/International Committee for Information Technology Standards (ANSI/INCITS) Technical Committee M1, Biometrics, que también actúa como el ANSI's Technical Advisory Group para el ISO/IEC Joint Technical Committee.
- ISO/IEC. International Standards Organization/International Electrotechnical Commission (ISO/IEC) JTC 1/SC 37 on Biometrics.
- NTSC. US National Science & Technology Council (NSTC) Subcomité de Biometría y Gestión de Identidades. Se ha establecido que las iniciativas biométricas del gobierno de Estados Unidos se basarán en los estándares biométricos del ANSI/INCITS y del ISO/IEC.
- UK British Standards Institute (BSI). Agencia Nacional de Estándares de Reino Unido. Colabora con el UK's Technical Advisory Group para el ISO/IEC Joint Technical Committee.
- ICAO. United Nations International Civil Aviation Organization (ICAO) establece los estándares de integración de la biometría en los pasaportes electrónicos de acuerdo con el INCITS y el ISO/IEC.
- NIST. The US National Standards Institute. Agencia Estadounidense que desarrolla los estándares técnicos del gobierno, incluyendo aquellos que afectan a tecnologías biométricas. Los estándares del NIST se establecen de acuerdo a los del INCITS y del ISO/IEC.

La totalidad de estos estándares reconocen como un método seguro, eficiente y de fácil integración, a los Sistemas de Control de asistencia basados en huella dactilar [29].

1.10. Consideraciones finales del capítulo

Las características biométricas son los elementos más seguros para la autenticación de una persona. Los sistemas biométricos constituyen hoy una alternativa confiable para la implementación de la seguridad en empresas y entidades. Las técnicas biométricas de seguridad son muy variadas, y de disímiles características, formando parte de cada sistema biométrico específico, acorde a las necesidades de los clientes y a la rama de la economía o la sociedad donde sean aplicadas. Por otra parte, los sistemas biométricos basados en huellas dactilares son los más extendidos en su uso, y dadas las características y procesamiento de la huella, son sistemas altamente efectivos, con parámetros para medir su exactitud claramente definidos. Una de las aplicaciones empleadas en los sistemas de huella dactilar la constituye el control de asistencia, la cual forma parte del objetivo central de este trabajo.

CAPÍTULO 2. Diseño de un sistema biométrico de control de asistencia

2.1. Introducción

Como se planteó en la introducción de este trabajo resulta necesario para la Empresa de Telecomunicaciones de Cuba (ETECSA) tener un control estricto del personal que labora en la misma y para ello se ha decidido crear un sistema biométrico de control de asistencia basado en huella dactilar.

Este sistema tendrá los siguientes requisitos funcionales:

- Controlar la entrada/salida del personal que labora en las diferentes instalaciones de la empresa.
- Emitir reportes relativos a la asistencia, tiempo de trabajo, ausentes, etc.

Como requisitos no funcionales del sistema se plantean los siguientes:

- Cumplir con estándares internacionales previstos para estos sistemas.
- Utilización de un hardware que manipule las huellas dactilares.
- Utilización de un software especial para el reconocimiento de las huellas dactilares.

A partir de estos elementos se propone en este capítulo un Sistema Biométrico de Control de Asistencia personalizado a las necesidades de la empresa y para ello se presentan los siguientes elementos determinantes en este diseño:

- Estándares internacionales a tener en consideración

- Determinación del hardware a utilizar a partir del análisis de los más comunes en el mercado.
- Determinación del software, tomando como base los presentes en el mercado y el hardware elegido.
- Diseño de una aplicación personalizada que cumpla los requerimientos de la administración.
- Instalación y puesta a punto del sistema.
- Requisitos mínimos del sistema.
- Instalación del software a emplear.
- Principales riesgos del sistema.

2.2. Principales estándares a tener en cuenta para el diseño

Los principales estándares existentes implicados en los sistemas biométricos basados en huella dactilar son los que aparecen en la Tabla 2.1:

Tabla 2.1: Estándares Biométricos basados en huella dactilar.

Aspecto	Estándares
Imagen de la huella dactilar	ISO/IEC 19794-4 Formatos de intercambios de datos biométricos. Parte 4: Información de imagen facial.
	ASNI INCITS 381-2004 Formato de intercambio de información del dedo.
Minucia de la huella dactilar	ISO/IEC 19794-2 Formatos de intercambio de datos biométricos. Parte 2: Información de la minucia de la huella dactilar.
	ANSI INCITS 378-2004 Formato de la minucia del dedo para intercambio de datos.

	ANSI INCITS 377-2004 Formato de intercambio de la información básica del patrón dedo.
Generales	ANSI/NIST ITL 1-2000 Formato de la información para el intercambio de huella dactilar, facial cicatrices y tatuajes (SMT).
	INSI/NIST ITL 1-2007 Formato de la información para el intercambio de huella dactilar, facial y otro tipo de datos biométricos-Parte 1.
Interfaces técnicos	ISO/IEC 19784-1 BIOAPI- Interfaz de programación de la aplicación biométrica – Parte 1: Especificación BioAPI.
	ISO/IEC 19784-2 Interfaz de programación de la aplicación biométrica (BioAPI) – Parte 2: Interfaz del proveedor del archivo biométrico.
	ISO/IEC 19785-1:2006: Marco común de intercambio de formatos biométricos- Parte 1: Especificación de los elementos de la información.
	ISO/IEC 19785-2: 2006: Marco común de intercambio de formato biométricos- Parte 2: Procedimientos para la autorización de registros biométricos.
	ANSI INCITS 358-2002 Especificación BioAPO (Versión 1.1).
	ANSI INCITS 398-2005 [NISTIR 6529-A]. Marco común de intercambio de formatos biométricos. (CBEFF)
Rendimiento	ANSI INCITS 409.1-2005 Reporte y testeo del rendimiento biométrico-Parte 1: Principios y marco.
	ANSI INCITS 409.2-2005 Reporte y testeo del rendimiento biométrico. Parte 2: Reporte y testeo de la tecnología.
	ANSI INCITS 409.3-2005 Reporte y testeo del rendimiento biométrico. Parte 3: Reporte y testeo del escenario.

	ANSI INCITS 409.4 Reporte y testeo del rendimiento biométrico. Parte 4: Metodologías de la operativa de testeo.

Tomando como base este marco regulatorio es que se realiza el diseño del Sistema Biométrico para el control de asistencia que se expone a continuación [30].

2.3. Descripción y evaluación del hardware a utilizar

Para realizar el diseño de un sistema biométrico, se deben tomar en cuenta muchos factores antes de adquirir cierto dispositivo biométrico, tales como:

- Resolución
- Área del sensor
- Número de Píxeles
- Profundidad de color
- Calidad de imagen

Resolución: Indica los dpi (número de puntos o píxeles por pulgada), siendo 500 dpi la mínima resolución para tener un buen producto, sin embargo, es probable que un algoritmo pueda identificar las minucias en los modelos de las huellas capturadas con resoluciones de hasta 300 o 250 dpi.

Área del sensor: Es muy importante puesto que cuanto más grande es, mayor es el número de valles y protuberancias que se van a encontrar para poder hacer el posterior análisis. Una medida óptima para poder capturar todo el dedo es de 1 x 1 pulgadas cuadradas. Pero mientras más grande es esta área el precio también se incrementa.

Número de píxeles: Este valor es simplemente la multiplicación de la resolución (en dpi) a la que se está trabajando y el área (altura x ancho).

Profundidad de color: En el caso de trabajar con huellas digitales, los colores no son considerados necesarios y solamente se requiere niveles de grises, entonces este valor se puede denotar como el número de bits usados para codificar el valor de cada píxel. Un valor estándar es el de 8 bits (que nos permite alcanzar hasta 256 niveles de grises).

Calidad de imagen: Cuando los dedos están secos o mojados, o tienen cortes, o las protuberancias son poco profundas, la calidad de la imagen es pobre por lo que se debe considerar lectores con ciertas habilidades.

Es necesario conocer algunas características de los equipos biométricos para captura de huellas dactilares que han sido objeto de estudio para la presente implementación.

En la siguiente Tabla 2.2 se muestran estas características. Hay que considerar que la capacidad de usuarios sugerida en la tabla está tomada en cuenta en torno a un solo aparato, y con un software de aplicación se puede ampliar esta capacidad. En el caso de la aplicación sugerida, esto podrá variar de acuerdo a la cantidad de aparatos que se adquirirán.

Tabla 2.2: Tabla comparativa de equipos biométricos comerciales

Fabricante o Comercializador	**Modelo**	**Costo**	**Resolución en dpi**	**Capacidad de usuarios**	**Software desarrollo**
Superma	BioEntry Pass	$780.00	500	9000 a más con software	SI
JcTechnologies Systems SAC	Fingermatch FM-200U	$980.00	500	9000 a más con software	SI
Sagem Défense Sécurité	Morphosmart: Licencias: VerifMorphoSoft IdentLiMorphosoft IdentPlus	$795.00 $1109.00 $5048.00	500	20000 a más con software	SI
SynoBiometrix	BSS-1B	$720.00	513	99	
Sagem Défense Sécurité	MorphoAccess MA200	$1883.77	500	800 sin software, 48000 con software	SI
Secugen Corporation	Secugen Hamster IV	$598.00	500	1000	SI
Digital Persona	4000B Reader	$600.00	512	1000	SI

BioIndentidad CA	BioStart SDK	$670.00	500	1000	SI
Jc Technologies Systems SAC	Finger 007	$1550.00	500	4500	SI
Biometrix INT	FM-FC	$1900.00	500	9000	SI
Jc Technologies Systems SAC	MagicPrint 4500	$1330.00	500	90	
Jc Technologies Systems SAC	BF 660C	$1100.00	500	250	
Biometric International	FIM01	$1500.00	500	1000, 2000, 4000	SI
Bometría Aplicada	U4000B	$89.00	512	20	
Hit Corporation	Magic Plus 4200	$1000.00	500	500, 1000	
D2 Technology Limited	Finger Pass KF-2000	$308.00	500	1000, 4000	
Granding Technology Co.	X628	$308.00	500	1500	
Granding Technology Co.	Biosh-F7	$374.00	500	500	
BioEnable Technologies	iScan V100	$350.00	500	100	
BioEnter International Inc	BFS 310	$449.00	500	99	
D2 Technology	BioSH-TA2	$493.00	500	1000	

A continuación se detallan algunos productos de interés según el tipo de solución planteada anteriormente [31].

2.3.1. BioEntry Pass

Los equipos Bioentry Pass están diseñados para la aplicación requerida. Consiste en la validación de acceso por huella dactilar exclusivamente. El equipo puede acumular hasta 9000 plantillas de huellas para reconocimiento. Pero conectados a un servidor de validación, es posible llegar a cantidades mayores. En red el tiempo promedio de reconocimiento 1:1000 es de aproximadamente 1 segundo. El costo de cada equipo, con lector FC (de barrido de huella) es de $600.00. En el caso de que se requiera el software de desarrollo, se puede adquirir un BioEntry Pass SK que incluye un equipo, soporte y software SK con rutinas en C++ y aplicaciones desarrolladas por $ 780.00. Este equipo se muestra a continuación en la Figura 2.1 [32].

Figura 2.1: Lector de huella dactilar, BioEntry Pass

2.3.2. Lector de huella digital FM-200U

El lector de huella dactilar FM-200U presenta un software de verificación dactilar que permite, en una primera fase, registrar los datos y huella digital de cada empleado, los ya existentes y también personal nuevo que vaya ingresando. Cuando los empleados empiecen a llegar deben introducir un código en el teclado de la PC y luego colocar su huella en el lector, si la verificación es correcta se generará una marcación con nombre, fecha y hora. Si la verificación es incorrecta, el sistema pedirá se ingrese nuevamente el código. El precio

de este aparato es de $650.00 incluido IGV y el Kit de desarrollo $980.00. El lector de huella dactilar FM-200U se muestra en la Figura 2.2.

Figura 2.2: Lector de huella dactilar FM-200U

Sus características son:

- Sensor óptico de huella digital CMOS/Microprocesador ASIC integrado
- Resolución óptica: 500 dpi niveles de grises
- Conexión a PC por puerto USB
- Tamaño de la minucia - 256 bytes
- Plataformas de operación WIN98/2000/XP
- No es compatible con el modelo FM100U
- Operación en Modos de Verificación e Identificación
- Comunicación hacia la PC por Puerto USB
- Licencia de uso: Licencia única sin límite en el número de huellas.
- Interfaz de Programación: Vía DLL
- Capacidad de integrarse con redes Ethernet permite su conexión a plataformas NOVELL, WIN 95, WINDOWS NT, UNIX., ORACLE.
- Validación remota: Valida el acceso de los usuarios remotos por Internet, Intranet, Extranet o por Red Privada Virtual (VPN) como si estuvieran ubicados localmente. Esta aplicación es disponible mediante desarrollo usando SDK.

Este producto también cuenta con un Kit de desarrollo, para poder trabajar con un mayor número de personas, se puede programar en Visual Basic, visual C++, a través de DLL. El precio total del producto estaría alrededor de los $650.00 [32].

2.3.3. MorphoSmart MSO30

Este producto es desarrollado y producido por Sagem Défense Sécurité, el líder mundial en sistemas de identificación de impresiones dactilares. El MorphoSmart MSO300 es un escáner de captura de huellas dactilares preciso, compacto, durable y fácil de integrar en aplicaciones de identificación automática de las impresiones dactilares, el cual se muestra en la Figura 2.3.

Figura 2.3: Lector de huella dactilar MorphoSmart MSO300

El MorphoSoft es compatible con las plataformas de programación Active X de Windows, lo cual permite integrarlo fácilmente en aplicaciones de registro, autenticación e identificación automática de personas. El entorno de programación cumple con las normas técnicas BioAPI, optimizando los tiempos de puesta en marcha de los proyectos. El MorphoSoft está disponible en diversas licencias biométricas diferenciadas, que permiten hacer procesos de verificación (1:1) e identificación (1: N). Por ejemplo, la licencia identificación automática (1: N) MorphoSoft IdentPlus permite identificar a una persona entre 20,000 personas con sólo poner el dedo en tiempos extremadamente cortos; típicamente menores a 1 segundo en una computadora convencional.

Al hacer un análisis de estos productos se constata que no son hechos para trabajar con grandes volúmenes, salvo uno (el MorphoSmart MSO300); en cambio si se quisiera trabajar con grandes volúmenes se deberá usar un software especial [32].

2.3.4. Morpho Access MA20

Este producto, al igual que el Morphosmart MSO300 es desarrollado y producido por Sagem Défense Sécurité, por lo que presenta las mismas prestaciones y se muestra en la Figura 2.4.

Figura 2.4: Lector de huella dactilar MA20

Algunas características que pueden ser resaltadas son:

- Sistema biométrico más rápido y preciso del mundo.
- Identifica al trabajador y registra su hora de marcación con sólo poner el dedo (no requiere códigos o tarjetas).
- Registra la fecha, hora y datos del trabajador para cada marcación.
- Soporta dedos en malas condiciones (con sequedad, humedad, cicatrices, suciedad, etc.).
- Altamente tolerante a la mala posición del dedo (rotación y traslación).
- Es fácilmente integrable con cualquier sistema informático de control de asistencia.
- Permite diferenciar cuatro tipos de eventos de asistencia (entrada, salida, entrada intermedia y salida intermedia).
- Cuando identifica al trabajador permite abrir una puerta automáticamente.

El MorphoAccess está dotado con comunicación Ethernet TCP/IP, lo cual permite descargar los reportes relativos a la asistencia (ingresos y salidas del personal) directamente a través de la red. Asimismo, cuenta con múltiples interfaces de comunicación adicionales como RS-232 (serial), RS-422, Wiegand, etc. En forma complementaria, el MorphoAccess contiene un controlador de puerta incorporado, que permite la apertura automática de una puerta, sea esta eléctrica o magnética [32].

2.3.5. Secugen Hamster IV

El escáner de huella digital Hamster IV cuenta con la industria del sensor óptico más robusta y avanzada, ya que utiliza la tecnología patentada de huella digital biométrica de superficie de reflexión. El escáner de huella dactilar tiene una función de encendido automático, que automáticamente comprueba la presencia del dedo. Además, posee una función de captura inteligente que asegura la calidad del escaneo de las huellas dactilares, ya que ajusta automáticamente el brillo de la imagen. El lector de huella dactilar Secugen Hamster IV se muestra en la siguiente Figura 2.5 [33].

Figura 2.5: Lector de huella dactilar Secugen Hamster IV

Las características principales de este dispositivo se muestran en la Tabla 2.3.

Tabla 2.3: Características del Secugen Hamster IV

Característica	Detalle
Dimensiones	Ancho: 2,7 cm Largo: 4 cm alto:7,3 cm
Peso	100 g.
Resolución	500 dpi
Tiempo de verificación	Menos de 1 segundo
Tipo Captura	Óptico, permite realizar la adquisición de la imagen en formato jpg o string.
Interfaz	USB
Sistemas Operativos soportados	Windows 7 / Vista/ Server 2003 / Xp / Milenium / 98.
Certificaciones	Comisión general de comunicaciones (FCC)[11] y Restricción de ciertas Sustancias Peligrosas en aparatos eléctricos y electrónicos (RoHS)[12].
Otros	Dispositivo Biométrico con librerías SDK. Compatible con Java.
Estándares soportados	Intercambio de datos basado en minucias ISO 19794-2 y INCITS 378. BioApi[13].

2.3.6. 4000B Reader

Estos lectores utilizan la tecnología de exploración óptica de huellas digitales, para lograr una excelente calidad de imagen y una amplia área de captura. Poseen una capacidad de autenticación precisa y rápida, incluso de las huellas dactilares irregulares, sin importar el ángulo de colocación. El lector puede ser utilizado para integrar aplicaciones desarrolladas. Este lector se muestra a continuación en la Figura 2.6 [34].

Figura 2.6: Lector de huella dactilar 4000B Reader

Sus características principales se muestran en la Tabla 2.4 que aparece a continuación.

Tabla 2.4: Características del 4000B Reader

Característica	Detalle
Dimensiones	Ancho: 6,0 cm Largo: 10,3cm Alto:5,8 cm
Peso	120 g.
Resolución	512 dpi
Tipo Captura	Óptico, permite guardar la imagen en formato jpg.
Tiempo de verificación	Menos de 1 segundo
Interfaz	USB
Sistemas Operativos soportados	Windows 7 / Vista/ Server 2003 / XP y Windows Server 2000 y 2003
Certificaciones	FCC Clase B
Otros	Dispositivo Biométrico con librerías SDK, previo registro. Rechazo de huella latente, Rechazo de huella falsificada
Estándares soportados	USB, WHQL[15]

2.3.7. Biostart SDK

El dispositivo Biostart SDK contiene un kit de desarrollo de software para el control de acceso del personal, ya que permite manejar las funciones de autenticación e identificación. Esto hace posible la integración del hardware con cualquier software de control de asistencia. El kit incluye las librerías (DLL), soporta para los lenguajes de programación (Visual Basic, Visual C++, C#). El Biostart SDK se puede apreciar en la Figura 2.7.

Figura 2.7: Lector de huella dactilar Biostart SDK

Sus características se muestran en la Tabla 2.5.

Tabla 2.5: Características del Biostart SDK

Características	Detalle
Tamaño	Ancho: 5,0 cm Largo: 16 cm Alto:3,7 cm
Resolución	500dpi
Velocidad	2000 comparaciones en 1 segundo
Tarjeta RF	125KHz(EM,HID)
Tipo Captura	Óptico permite almacenar la información de las huellas en el dispositivo. Máximo 1000 huellas.
Modos de Operación	Huella, Tarjeta, Huella – Tarjeta
Interface	TCP/IP, RS485
Otros	Soporta diversos lenguajes de programación (Visual Basic, Visual C++, C#)

Existe gran variedad de dispositivos biométricos para el control de asistencia basados en huella dactilar, con diferentes características y funcionalidades, ejemplo de los cuales se pueden apreciar en el Anexo 2 [34].

2.3.8. Decisión

Teniendo en cuenta que la cantidad de empleados de la División Territorial de ETECSA Matanzas es de190 trabajadores, el costo del equipamiento y las funcionalidades de los mismos, se seleccionan los siguientes equipos que se muestran en la Tabla 2.6.

Tabla 2.6: Tabla comparativa de equipos biométricos

Característica	SECUGEN HAMSTER	4000B READER	BIOSTAR SDK
Resolución	500 dpi	512 dpi	500 dpi
Tipo Comunicación	USB	USB	Ethernet
Autenticación	Remota	Remota	Local
Lenguajes soportados	Visual Basic, C#, java	Lenguaje C#	Visual basic, visual C++, C#
Formatos de almacenamiento de datos	JPG o String.	JPG	JPG, almacenamiento en el dispositivo
Lector	Óptico captura automática	Óptico	Óptico, captura automática

De estos tres equipos se identifica que el Secugen Hamster es el hardware más robusto, puede almacenar la información de la huella en dos formatos diferentes y posee lector óptico con captura automática. Además tiene una más fácil interacción con los distintos lenguajes de programación, tales como Visual Basic, C# Sharp y Java. Todos estos elementos hacen de este hardware el más completo para realizar la implementación del sistema biométrico. Se toma en cuenta además, que con la empresa fabricante, la cual es europea, con sucursales en varios países de América (incluyendo Venezuela), es factible el intercambio comercial con Cuba. Profundizando aún más en las características del dispositivo seleccionado, en la siguiente Tabla 2.7 se muestran las características específicas del lector Secugen Hamster.

Tabla 2.7: Características específicas del SecugenHamster

Fingerprint Sensor	SecuGen USB Sensor
Dimensions (w/o stand)	1.1" x 1.6" x 2.9" (27 x 40 x 73 mm)
Weight (w/o stand)	3.5 oz. (100 g)
Resolution	500 dpi ± 0.2%
Verification Time	Lessthan 1 second
OperatingTemperature	32° to 104°F (0° to 40°C)
OperatingHumidity	< 90% relative, non-condensing
Interface	USB 1.1, 2.0
SupportedOperatingSystems	Windows 7 / Vista / Server 2003 / XP / 2000 / Me / 98 SE.
Certifications	FCC, CE, RoHS

Nombre Scanner	Lector de huella digital SECUGEN HAMSTER PLUS
Fabricante	SecuGen Corporation
Conexión	USB 2.0
Voltaje de operación	5 V + 5 %
Potencia (máxima)	450 mW
Corriente (máxima)	99 mA
Sensor	Óptico FDU03FRS
Longitud del cable	1800 mm
Sistemas operativos	Windows 7/Vista / 2003 / XP / 2000 / Me / 98 SE
Resolución	500 dpi
Área para capturar imagen	16 x 18 mm (0.6" x 0.7")
Tamaño de la imagen	260 x 300 pixeles
Imagen en escala de grises	256 tonos (8-bit escala de grises)
Distorsión (no lineal)	< 0.1 %
Iluminación	Led Rojo
Tamaño del dispositivo (sin soporte)	27 x 40 x 73 mm (1.1" x 1.6" x 2.9")
Peso del dispositivo (sin soporte)	100 gramos
Temperatura de operación	0°C ~ +40°C
Humedad de operación	0-90 % (sin condensación)
Velocidad de comunicación (máxima)	12 Mbps
Velocidad de captura de imagen	0,2 segundos
Certificación de cumplimiento	FCC[23], CE[24], RoHS[25]

En la Figura 2.8 que se muestra a continuación, se puede constatar el dispositivo seleccionado en este trabajo: El SecugenHamster [33].

Figura 2.8: Dispositivo Secugen Hamster

2.4. Descripción y evaluación del software a utilizar

Seleccionado el hardware que sea capaz de capturar la huella dactilar, tanto para el almacenamiento de las mismas, como para la identificación/verificación, es necesario elegir el software especializado que permita la comparación de la huella recogida con las huellas almacenadas en la base de datos. Estos programas utilizan algoritmos de comparación complejos y que son, en última instancia, los que determinan la efectividad de la propuesta.

A continuación se describen algunos de los software más utilizados en la actualidad y seguidamente se selecciona uno de ellos:

Fingerprint SDK

Fingerprint SDK es un software innovador, que permite integrar la biometría a un amplio rango de aplicaciones, gracias a su soporte para docenas de lenguajes de programación, riqueza en el código de los ejemplos y su documentación completa. Fingerprint SDK está disponible en dos diferentes versiones. Fingerprint SDK para Windows soporta muchos lenguajes de programación a través de DLL, Java, ActiveX o .NET. Fingerprint SDK para Java permite el desarrollo multiplataforma de programas en Java que funcionan en Microsoft Windows o en Gnu/Linux. El principal objetivo es permitir el desarrollo de aplicaciones personalizadas tales como sistemas de autorización, sistema de transacciones, tiempo de atención, identificación en puntos de venta y acceso físico a través de autentificación por huellas dactilares. Las especificaciones del Fingersprint se muestran en la Tabla 2.8 [35].

Tabla 2.8: Especificaciones del Fingerprint SDK

Plataforma	Fingerprint SDK para Windows: Windows 2000, Windows XP, Windows 2003, Windows Vista. Fingerprint SDK para Java: Windows 2000, Windows XP, Windows 2003, Windows Vista, Linux x86.
Requisitos mínimos de sistema	Procesador clase Pentium (i386) (200 MHz o superior) con 64Mb o mas, 20Mb de espacio de HD.
Velocidad de Identificación (1:N)	Fingerprint Identification SDK: hasta 35.000 huellas por Segundo. Fingerprint Verification SDK: 100 huellas por Segundo.
Velocidad de Verificación (1:N)	10 milisegundos.
Velocidad de extracción de templates	100 milisegundos.
Tamaño del Template	900 bytes (promedio).
Bases de datos	Fingerprint SDK no utiliza ningún sistema de base de datos en particular. Los templates son entregados a la aplicación integradora que debe almacenarlos de la forma decidida por el programador.
Resolución de la Imagen	Recomendada: 500 DPI Mínimo: 125 DPI Máximo: 1000 DPI
Tamaño de la imagen	Mínimo: 50x50 pixels Máximo: 500x500 pixels

Verifinger SDK

Uno de los softwares de mayor utilización en los equipos biométricos es el Verifinger SDK, y está previsto para sistemas biométricos de desarrollo e integración. Este permite un desarrollo rápido de la aplicación biométrica usando funciones de Verifinger DLL o de la misma librería de Verifinger, el cual asegura una alta confiabilidad en la identificación de la huella digital en los modos de 1:1 y 1:N y una velocidad de comparación de 30,000 huellas digitales por segundo. Verifinger puede ser fácilmente integrado al sistema de seguridad del cliente.

El integrador tiene un control completo sobre las entradas y salidas de la data del SDK. Es por ello que las funciones del SDK pueden ser usadas en conexión a cualquier scanner, usuarios de interfase o base de datos.

Existen varios tipos de Verifinger 4.2 SDK:

- Verifinger 4.2 Standard SDK: Provisto para la mayoría de sistemas biométricos que desarrollan y permiten el uso de aplicaciones biométricas de Windows o Linux. Incluye una licencia para Verifinger 4.2 DLL/ instalación en biblioteca, Módulo de integración para MySQL (para Linux), uso de la biblioteca para aplicaciones de la muestra de Verifinger con códigos de fuente (para Windows y Linux), conductores de exploración de la huella digital y software de documentación.
- Verifinger 4.2 Extended SDK: Provisto para quienes les gustarían empezar con un desarrollo rápido de su red de sistema biométrico cliente/servidor. Incluye todas las características del Verifinger 4.2 Standard SKD, además incluye 3 Verifinger DLL/licencia para la instalación de biblioteca, componentes Active X para el desarrollo de cliente/servidor (sólo para MS de Windows) y componentes para el uso de la muestra de aplicación (con códigos de fuente).
- Verifinger 4.2 Library SDK: Provisto para proyectos de biometría grandes. Este SDK contiene bibliotecas de Verifinger para Windows y Linux sin protección para la copia, ¨Verifinger 4.2 Paquete del código fuente¨también está disponible y contiene ¨Verifinger 4.2 código fuente de algoritmos y documentación¨. El código fuente de Verifinger 4.2 está escrito en ANSI C de manera bien estructurada y documentada [35].

Existen otros softwares de desarrollo tales como:

- MegaMatcher SDK
- FingerCell EDK
- VeriLook SDK

Dadas las características antes mencionadas de los softwares existentes (propietarios), se toman en consideración los siguientes requerimientos para el sistema biométrico de control de asistencia: Se ajusta para el desarrollo de aplicaciones personalizadas (como la que se propone más adelante), fácil implementación, soporte para docenas de lenguajes de programación y no utiliza ningún sistema de base de datos en particular, sino que esto queda a criterio del programador; sobre esta base se selecciona el Fingerprint SDK como software para el sistema de control de asistencia propuesto.

Tomando como base el Fingerprint SDK, incluido en el dispositivo SecugenHamster IV seleccionado, se realiza además el diseño de una aplicación más personalizada, que permita a partir de la identificación del empleado mediante la huella dactilar, llevar los registros horarios de asistencia, datos de cada trabajador y elaboración de reportes útiles que permitan la gestión eficiente de la asistencia del capital humano por parte de la empresa.

Además del software específico escogido para la identificación/verificación de la huella dactilar es necesario determinar el lenguaje de programación y el gestor de datos que se utilizarán en la aplicación personalizada a diseñar. Se escogieron el lenguaje PHP y el gestor de datos SQL Server, cuyas características esenciales se describen a continuación:

PHP

Es un lenguaje interpretado del lado del servidor, que se caracteriza por su potencia, versatilidad, robustez y modularidad. Los programas escritos en PHP son embebidos directamente en el código HTML, y ejecutados por el servidor WEB a través de un intérprete antes de transferir al cliente que lo ha solicitado un resultado en código HTML puro.PHP posee varias características que lo hacen indicado para el software que se implementa, de las cuales se pueden mencionar las siguientes:

- Orientado al desarrollo de aplicaciones web dinámicas con acceso a información almacenada en una base de datos.

- El código fuente escrito en PHP es invisible al navegador web y al cliente, ya que es el servidor el que se encarga de ejecutar el código y enviar su resultado HTML al navegador. Esto hace que la programación en PHP sea segura y confiable.
- Capacidad de conexión con la mayoría de los motores de base de datos que se utilizan en la actualidad, destaca su conectividad con MySQL y PostgreSQL.
- Es libre, por lo que se presenta como una alternativa de fácil acceso para todos y reduce los costos para la empresa que desee una herramienta informática para sus procesos.
- Permite aplicar técnicas de programación orientada a objetos ideales para el software a desarrollar.
- Soporta el manejo de excepciones [36].

MySQL Server

MySQL Server es un sistema de gestión de bases de datos relacionales para soluciones de almacenamiento de datos necesario para aplicaciones de negocio, comercio electrónico, etc.

Algunas de las características más importantes que posee MySQL Server son las siguientes:

- Los clientes se conectan al servidor MySQL Server usando sockets TCP/IP en cualquier plataforma.
- Seguridad: ofrece un sistema seguro de contraseñas y privilegios mediante verificación basada en el host, y el tráfico de contraseñas está cifrado al conectarse a un servidor.
- Soporta gran cantidad de datos. MySQL Server tiene bases de datos de hasta 50 millones de registros.
- Se permiten hasta 64 índices por tabla. Cada índice puede consistir desde 1 hasta 16 columnas o partes de columnas. El máximo ancho de límite son 1000 bytes [37].

2.5. Características de la aplicación

Para el diseño de la aplicación no es necesario profundizar en el funcionamiento interno del dispositivo biométrico seleccionado (Secugen Hamster IV), razón por lo cual se omite su descripción. Sí resulta necesario el análisis de la forma en que se captura la imagen para posteriormente vectorizarla y generar su código, el cual se genera internamente por el manejador del dispositivo: La captura se realiza al presionar el dedo sobre la parte sensible y una vez detectada la presión sobre él se realiza el escaneo.

Una vez realizado el escaneo se genera un código de 61 dígitos que será de ahora en adelante el código para el reconocimiento de la huella digital (plantilla de huella) que se capturó.

Estos 61 dígitos representan la interpretación de todos y cada uno de los elementos que integran a la huella digital capturada.

Una vez obtenido este código, se puede almacenar en una base de datos para su posterior uso en la identificación de personas. La forma en que se realiza la captura de dicho código es: obtener un código que sea real, se debe tomar una muestra de la huella dactilar, de esta muestra se obtiene un código que es el más aproximado posible al de la huella escaneada. Una vez obtenido dicho código, solo resta hacer la verificación y para esto solo se toma la muestra a comparar contra el código capturado.

Para el desarrollo de este sistema, se creó una base de datos en MySQL Server, dentro de esta base se cargaron tablas con la información personal de los usuarios, para este caso los empleados de la empresa.

Los módulos de registro y verificación son los módulos esenciales de la aplicación

Módulo de registro:

Este módulo es el encargado de registrar los trabajadores, este proceso en un inicio se hace para todos los trabajadores de la empresa y luego se utiliza para cada nuevo trabajador que se incorpore.

Se ejecuta el módulo al elegir en el menú de opciones “Trabajador – Nuevo”, y entonces se ejecutan las siguientes acciones:

1-Preparación y captura de la muestra de huella dactilar.

2-Verificar que la imagen tenga una calidad alta.

3-Capturar los datos generales del trabajador.

4-Almacenar los datos.

En la Figura 2.9 se muestra el Modulo para registro de un trabajador.

Figura 2.9: Módulo para registro de un trabajador

Módulo de Verificación

Este módulo es el encargado de controlar la entrada/salida de los trabajadores y en esencia en él se realizan las siguientes acciones:

1-Captura de la huella dactilar.

2-Buscar el ID (código asignado a una huella especifica), en la base de datos.

3-Extraer de la base de datos, nombre y apellidos, departamento, cargo.

4-Poner asistencia (Fecha y hora de entrada/ Fecha y hora de salida)

El trabajador pone el dedo en el escáner, se detecta por el dispositivo y se realiza el escaneo de la huella dactilar, generando el código comentado, se analiza la calidad de la huella y se identifica el trabajador (ambas tareas realizadas por Fingerprint). Se almacena en la base de datos el registro sobre la fecha y hora de ingreso/salida

En la Figura 2.10 se muestra la pantalla para el registro de entrada y salida de un trabajador.

Figura 2.10: Registro de entrada y salida.

El software cuenta con otros módulos complementarios. Se presenta al usuario como se muestra en la Figura 2.11. En la cual se puede apreciar se que se listan los trabajadores por departamentos. Estos trabajadores pueden ser borrados del sistema o se pueden editar sus datos.

Figura 2.11: Aplicación para el control de asistencia

Además se puede observar que en el menú principal hay una opción denominada “usuarios” mediante la cual se gestionan aquellas personas que pueden acceder al sistema para su configuración general, denominadas administradores del sistema

La interfaz para la gestión de los administradores se muestra a continuación en la Figura 2.12.

Figura 2.12: Gestión de Administradores

Base de Datos

Como se ha especificado el sistema de almacenamiento, está basado en el gestor de datos MySQL Server y se utilizan dos bases de datos, la primera FingerDataBase y una segunda USRDataFinger.

La base de datos (FingerDataBase) es la interfaz lógica usada por el controlador para asignar una identificación a cada usuario. De allí se toma el número de identificación para enlazar a la base de datos de usuarios (plantilla de huella).

En la base de datos de usuarios (USRDataFinger) se encuentran dos tablas:

1-Tabla de registro de usuarios (usrfinger), contiene información en 14 columnas, la primera de ellas guarda el ID (código de usuario asignado para validarse, asignado por el software), otros campos son: nombre, apellidos, carne de identidad, departamento, cargo, fecha de registro.

2-Tabla de historial de accesos, en donde se registran cada uno de los eventos realizados por el usuario como fecha y hora de entrada, además del nombre, carne de identidad y cargo.

2.6. Instalación y puesta a punto

La instalación y puesta a punto del sistema se explica a continuación.

El sensor biométrico Secugen Hamster IV se instala en la puerta de entrada de la División Territorial de ETECSA en Matanzas, el cual estará conectado por vía USB a una PC para tales fines. En la Figura 2.13 se muestra la conexión local del sensor.

Figura 2.13: Conexión local

En el caso de la División Territorial de Matanzas, tiene una sola puerta de entrada para todos los empleados, pero este tipo de solución puede generalizarse si existen varias áreas administrativas, en cuyo caso pueden conectarse en red. Esta conexión en la red puede observarse en la Figura 2.14 que se muestra a continuación.

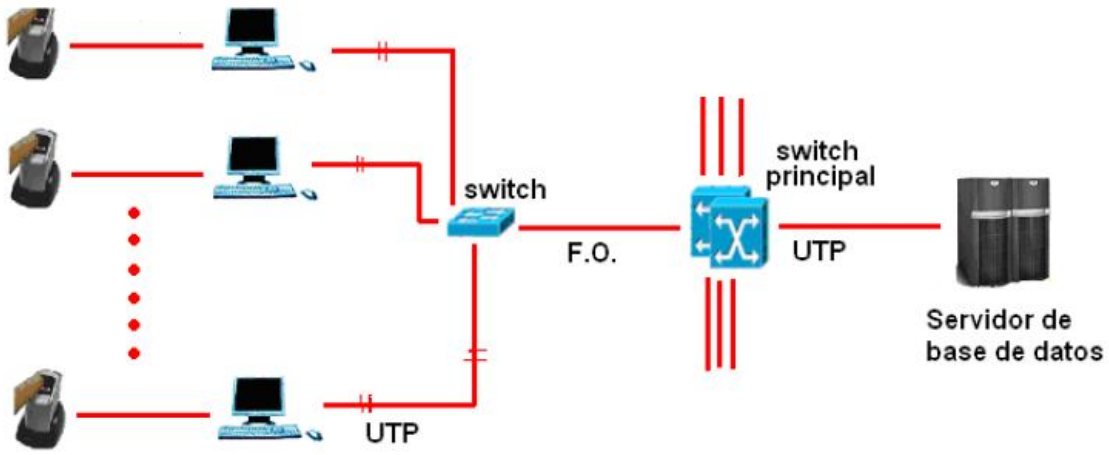


Figura 2.14: Conexión en red

Los empleados utilizan el sensor biométrico para la entrada y salida del Edificio Administrativo, lo cual es transparente para los mismos, ya que para cada entrada o salida, será identificado el empleado, así como la hora en que sucede el evento. El sensor será ubicado, tal y como fue mencionado anteriormente, en la puerta de entrada del Edificio de la División Territorial de ETECSA Matanzas, como se muestra en la Figura 2.15.

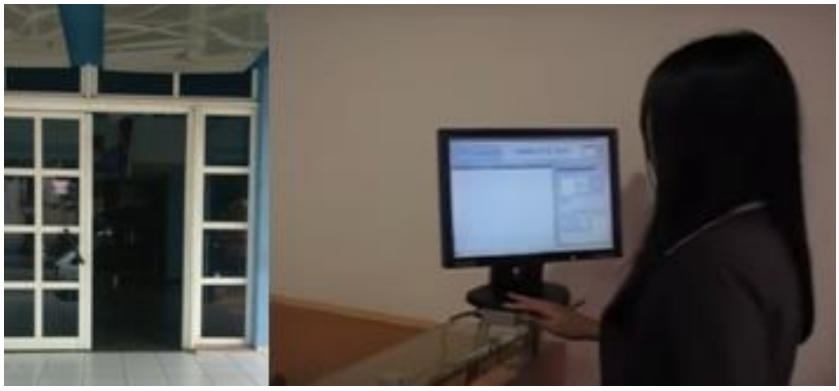


Figura 2.15: Lugar de instalación del sensor biométrico (puerta de entrada)

El sensor será instalado teniendo en cuenta las siguientes consideraciones:

- El dispositivo biométrico no debe ser colocado a la intemperie, eso dificulta su operación y durabilidad.
- El suministro de energía debe contar con tierra física, supresor de picos y batería de respaldo.
- Se debe colocar en la entrada principal, visible a todos los empleados.
- Debe estar a una altura tal que se encuentre al alcance de todos los empleados.

Los requisitos mínimos del sistema son:

- PC dedicada.
- Sistema operativo: Windows XP o superior.
- Procesador: Pentium IV o superior
- Memoria RAM: mínimo 1GB
- Espacio en disco duro: 20 MB para instalación
- Unidad de CD para la instalación
- Monitor: SVGA con resolución mínima de 1024X768
- Puertos USB: 1 puerto disponible para la conexión del lector biométrico.
- Puertos USB: Según las funciones adicionales del software:

1 puerto para llave de software (cuando el software va a operar en red con la licencia multiusuario).

1 puerto para Cámara Web (para captura de fotos de empleados y operadores)

- Tener instalado el software de control de acceso en la PC (Fingerprint SDK y software propuesto), y haber registrado a los empleados con su respectiva información.

Los pasos para instalar el software Fingerprint SDK en la PC son:

- Los drivers para el lector de huella USB se encuentran en la carpeta Drivers Lector USB BioMini del CD de instalación. Ejecute el archivo Sup_Fingerprint_Driver.exe

y cuando finalice la instalación conecte el lector de huella USB al computador. El sistema detectará un nuevo hardware y lo instala automáticamente. En la Figura 2.16 se muestra la pantalla de instalación del driver Secugen.

Figura 2.16: Instalación del driver SecuGen .

- Instalar el software de entradas y salidas con lector biométrico USB, ejecutando el archivo ZC500ESUSB_1.1.8.X_SETUP.exe ubicado en la carpeta ZC500ESUSB del CD de instalación. El instalador le irá enseñando paso a paso que es lo que debe hacer hasta finalizar la ejecución. En la Figura 2.17 se muestra el inicio del asistente de instalación del software Fingerprint SDK [38].

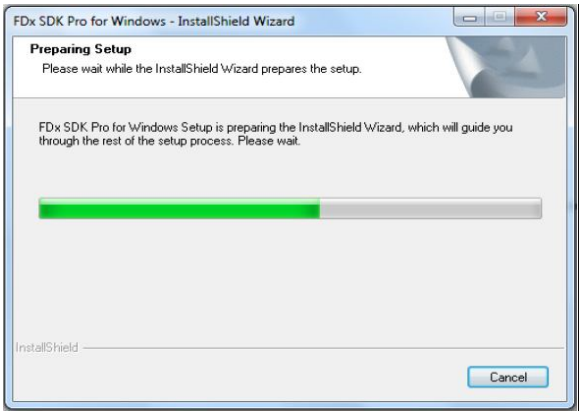


Figura 2.17: Inicio de Asistente de Instalación

La conexión USB del lector biométrico a la PC se muestra en la Figura 2.18.

Figura 2.18: Conexión USB del Lector Biométrico a la PC

2.7. Principales riesgos del sistema

El funcionamiento del sistema no debe verse afectado por ninguna configuración de hardware o software en particular, no obstante, se consideran riesgosos los siguientes procesos:

- Todas las instalaciones que pongan en riesgo a la computadora asociada al lector biométrico, como son, entre otras, las siguientes:
  a- Instalaciones eléctricas inseguras. No deben compartirse las conexiones con electrodomésticos (sobre todos los que producen arranques súbitos, como refrigeradoras, entre otros). Además se recomienda el uso de estabilizadores de voltaje y tomacorrientes con conexión a tierra.
  b- Promiscuidad, sobre todo de dispositivos tipo ¨flash memory¨ pues suelen ser fuente de contagio de virus y otras amenazas a la seguridad e integridad de la información.
  c- Falta de políticas de seguridad y administración del equipo. Se recomienda altamente la administración profesional del equipo, más allá del usuario común. Es deseable que la empresa cuente con personal calificado que discuta, aplique y garantice los resultados de políticas explícitas de seguridad para información. Por ejemplo, perfiles de usuarios, anti-virus, anti-spyware, etc.

- Cambio, eliminación, modificación de usuario(s) del sistema operativo. Sobre todo en Windows 7, se han suscitado problemas cuando se modifica el esquema de usuarios en el sistema operativo después de la instalación del software.
- Uso de máquinas virtuales. Este proyecto no ha sido probado en máquinas virtuales, por tanto, no se garantiza un correcto funcionamiento en tal entorno.
- Modificación del esquema de firewall y antivirus. En este caso no se garantiza el correcto funcionamiento del sistema si luego de su instalación se modifica la configuración de firewall de Windows u otros, así como de instalaciones de anti virus posteriores a la instalación del software.
- Si se colocan extensiones al cable de conexión USB del dispositivo Secugen Hamster Plus, no se garantiza el correcto funcionamiento de la solución. Se recomienda fuertemente que la máquina no se aleje del lector a una distancia mayor que la que el cable permite. Colocar extensiones es riesgoso porque en el mencionado caso, el lector no funciona correctamente.
- Tal vez el mayor riesgo para el buen funcionamiento del sistema es el uso del sistema por personal poco calificado. Es indispensable que se establezcan administradores que cumplan con los requisitos éticos y técnicos para el manejo del sistema. El administrador debe ser una persona de buen conocimiento informático y absoluta confianza de la empresa, de probada honestidad. Se debe considerar que: Un administrador de una sucursal puede alterar el reloj del sistema cuando la base de datos reside en el mismo equipo, lo cual genera que los reportes no se puedan obtener, a causa de inconsistencias en los datos; Un administrador puede alterar los reportes antes de enviarlos a la administración y un administrador puede atentar contra el funcionamiento del sistema por desidia, falta de cuidado en el uso, falta de limpieza, etc.
- Otro de los grandes riesgos es que el computador no cumpla con las características necesarias, a pesar de tener el sistema operativo, Office y demás elementos instalados según las recomendaciones.

2.8. Consideraciones finales del capítulo

El dispositivo Secugen Hamster IV es el lector biométrico de huella dactilar que se ha considerado idóneo a ser utilizado en el Sistema Biométrico de huella dactilar para el control de asistencia de los trabajadores de la Empresa de Telecomunicaciones de Cuba. Las prestaciones de este sensor entran en consonancia con el marco regulatorio vigente así como con sus características operativas, siendo de fácil adquisición en el mercado internacional. El software propietario Fingerprint SDK se torna como complemento al hardware seleccionado, ya que se ajusta al diseño propuesto y permite el desarrollo de una aplicación personalizada que posibilita llevar los registros horarios de asistencia, datos de cada trabajador y elaboración de reportes útiles.

CAPÍTULO 3. Funcionamiento y evaluación de los resultados

3.1. Funcionamiento

El primer paso para que el Sistema de Control de Asistencia Biométrico comience a funcionar, es el registro de los trabajadores en el mismo. Para esto se deben seguir los siguientes pasos:

- Ingresar los datos del trabajador: Nombre y apellidos, Departamento, Carne de Identidad, cargo.
- Posteriormente el usuario ingresa su huella para su posterior registro. La huella debe ser lo más nítida posible, sin embargo el sistema analiza la calidad y posición de la huella para darla como válida para su posterior guardado. Antes de que la huella sea guardada primero se verifica que la misma no exista ya dentro de la base de datos. La forma correcta de ubicar el dedo en el escáner puede ser apreciada en el Anexo 3.
- Si el sistema da por válido cada uno de los parámetros que se mencionaron anteriormente, la huella del cliente se guarda, sirviendo esta de base para futuras identificaciones al momento que se utilice el sistema. En las Figuras 3.1 y 3.2 se puede observar el proceso de lectura de la huella para su respectivo registro

Figura 3.1: Lectura de la huella para su respectivo registro

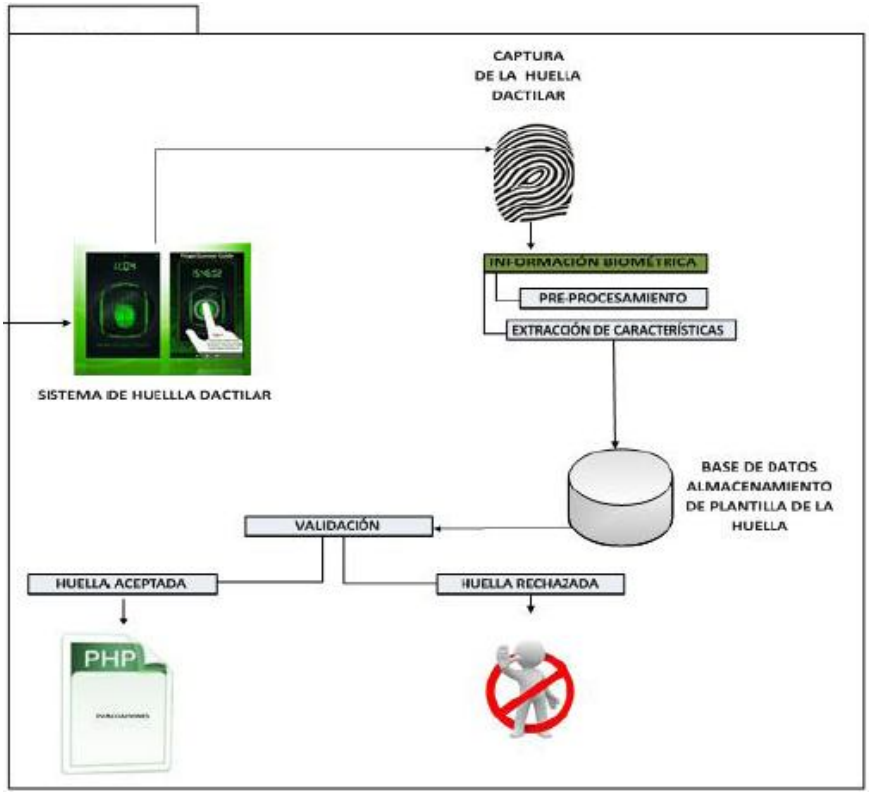


Figura 3.2: Funcionamiento de la Lectura de la huella para su respectivo registro

Cuando un trabajador ingresa en la Empresa, tendrá que registrar su entrada usando el hardware seleccionado, mediante el siguiente procedimiento:

- El sistema detecta el dedo en el sensor. Extrae automáticamente la plantilla de la huella. El sistema compara esta plantilla con la Tabla de trabajadores que constan registrados en el sistema. Si la plantilla coincide con una de las plantillas guardadas en el sistema, extrae el número de identificación correspondiente, y guarda la fecha y hora de entrada, y se muestra el siguiente mensaje ¨OK¨. En la Figura 3.3 se muestra el reconocimiento positivo.

Figura 3.3: Reconocimiento positivo

- Si la huella no fue procesada satisfactoriamente, el sistema lo hará saber con el siguiente mensaje ¨NO¨. En la Figura 3.4 se muestra el reconocimiento negativo.

Figura 3.4: Reconocimiento negativo

Cuando un trabajador sale de la Empresa, tendrá que registrar su salida usando el hardware seleccionado, mediante el siguiente procedimiento:

- El sistema detecta el dedo en el sensor. Extrae automáticamente la plantilla de la huella. El sistema compara esta plantilla con la Tabla de trabajadores que constan registrados en el sistema. Si la plantilla coincide con una de las plantillas guardadas en el sistema, extrae el número de identificación correspondiente, y guarda la fecha y hora de salida, y se muestra un mensaje ¨ OK¨.

• Si la huella no fue procesada satisfactoriamente, el sistema lo hará saber con el siguiente mensaje ¨NO¨. En las Figuras 3.5 y 3.6 se muestra la lectura de la huella para su respectivo ingreso o salida.

Figura 3.5: Lectura de la huella para su respectivo ingreso o salida

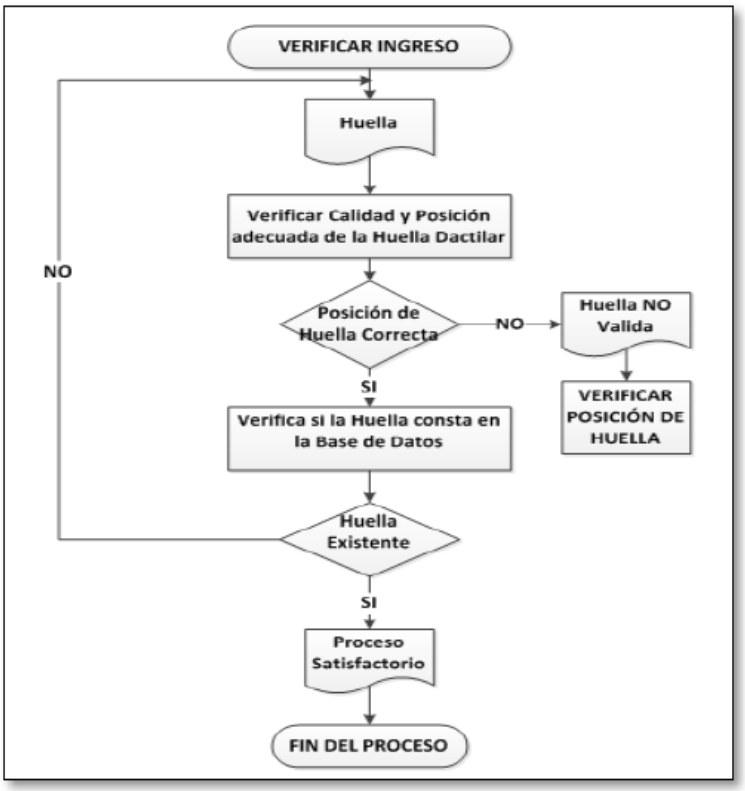


Figura 3.6: Funcionamiento de la Lectura de la huella para su respectivo ingreso o salida

Como se aprecia, el lector de huellas detecta los relieves del dedo mediante luz o sensores electrónicos, y tras detectar estos relieves crea una imagen digital a partir de los datos captados y la envía a la PC, donde será almacenada en una base de datos junto con los datos del trabajador correspondiente. Cuando la persona ya está almacenada en la base de datos, cada vez que ponga el dedo en el detector, será identificada, si por el contrario no está registrada el sistema dará un error como persona no identificada. En la Figura 3.7 se muestra simplificadamente el proceso de obtención de la imagen digital a partir de la huella.

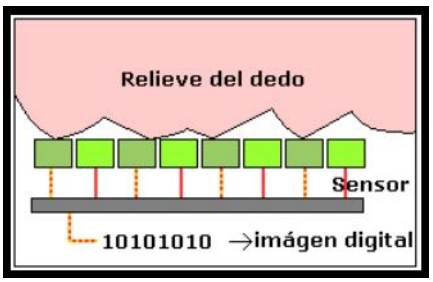


Figura 3.7: Obtención de la imagen digital

El sensor digitaliza el dedo del usuario y captura la imagen tridimensional de la huella dactilar. El algoritmo específico extrae puntos particulares de la imagen y convierte la información en un único modelo matemático, con 61 dígitos. Este modelo único se encripta y se archiva para representar a usuario. No se guarda ninguna imagen concreta de la huella dactilar.

Posteriormente, un usuario registrado posiciona el dedo en el sensor y una nueva imagen de la huella dactilar del usuario es capturada. Se extraen datos particulares de la huella dactilar y se convierten en una muestra. Esta muestra se compara a la muestra del usuario pre-registrada para comprobar la correspondencia. Si la muestra corresponde, el usuario es verificado positivamente.

En la siguiente Figura se muestra una imagen del Software Fingerprint para Secugen así como una pantalla del funcionamiento del sensor biométrico, lo cual se resume en lo expuesto anteriormente sobre los detalles de funcionamiento del sistema.

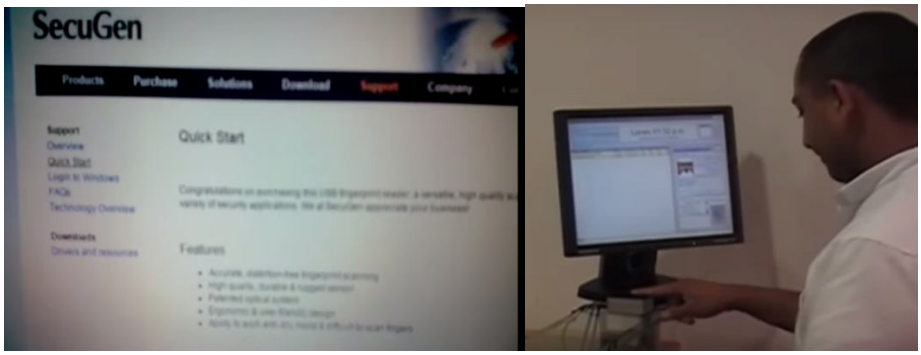


Figura 3.8: Detalles de funcionamiento.

3.2. Evaluación de los resultados

La bondad de un sistema biométrico depende drásticamente de muchas variables: la composición de la población (ocupación, edad, sexo, demografía, raza, entre otros), el entorno, el modo de hacer las pruebas, así como otras restricciones específicas de la aplicación. En una situación ideal, se querría caracterizar el rendimiento en un modelo independiente a la aplicación. Así, se podría predecir el rendimiento en una aplicación real.

Debido a la importancia de poder evaluar la precisión de los sistemas biométricos, se pueden definir tres tipos de evaluaciones:

- Evaluación de la tecnología: El objetivo es evaluar la calidad de los algoritmos dada una tecnología específica. No se evalúa todo el sistema sino algoritmo a algoritmo. Todos los algoritmos se comparan dados los mismos sensores, base de datos y cualquier aspecto que pueda afectar a los resultados. La base de datos se divide en dos partes. Normalmente, todos los datos se generan a la vez y la partición se lleva a cabo de una manera aleatoria. La primera parte compone la base de datos de aprendizaje (learningdatabase), y forma la parte de los datos que los usuarios

pueden usar para poder hacer la puesta a punto del algoritmo y extraer el máximo rendimiento. La segunda parte compone la base de datos de test (test database), y forma la parte de los datos que los evaluadores usan para hacer las pruebas finales. Los participantes no han podido usarla ni visualizarla antes de las pruebas. Debido a que los datos quedan disponibles para toda la comunidad científica, tras los experimentos se pueden repetir. Algunos libros de biometría incorporan DVD con estos datos. Es una evaluación repetible.

- Evaluación del escenario: El objetivo de este tipo de evaluación es determinar el rendimiento completo de todo el sistema en un prototipo de laboratorio o en un simulador de aplicaciones. El test se lleva a cabo en un sistema completo, pero en unas condiciones controladas aunque intenta simular una situación del mundo real. La comparación siempre se lleva a cabo con los mismos sensores biométricos y la misma población. Es una evaluación repetible.
- Evaluación del funcionamiento: El objetivo de esta evaluación es determinar el rendimiento del sistema completo en una situación real de entorno específico y una población específica. Es una evaluación no repetible debido a que puede haber parámetros no documentados o desconocidos. No hay una base de datos inicial [39].

Para la validación de las pruebas de funcionamiento y fiabilidad de la huella dactilar se deben tener en cuenta las tasas de falsa aceptación y falso rechazo, como se explicó en el primer capítulo.

Se emplearon 50 huellas dactilares diferentes para los procesos de registro y verificación, en total se obtienen 100 capturas de huellas dactilares de las cuales:

92 capturas fueron identificadas correctamente.

6 capturas no pudieron ser identificadas por el Sistema.

2 capturas no pudieron ser procesadas por la baja calidad que presentaba la huella.

0 capturas fueron identificadas incorrectamente por el sistema

Las huellas que no son tomadas en cuenta para el cálculo y análisis de las tasas son las 2 huellas que no fueron permitidas, ya sea por la baja calidad que presentaban o por la mala posición del dedo a la hora de la captura, siendo así se han tomado en cuenta 98 de las 100 huellas capturadas. Cabe recalcar que las 2 huellas que no fueron procesadas en la primera vez, tuvieron que volver a ser capturadas nuevamente de modo para que todos los usuarios puedan dar la evaluación. Los resultados obtenidos en el registro y verificación se muestran a continuación en la Tabla 3.1.

Tabla 3.1: Informe de pruebas

Usuario	Procesos	
	Registro	Verificación
Usuario 1	Aceptada	Aceptada
Usuario 2	Aceptada	Aceptada
Usuario 3	Aceptada	Aceptada
Usuario 4	Aceptada	Aceptada
Usuario 5	Aceptada	No Identificada
Usuario 6	Aceptada	Aceptada
Usuario 7	Aceptada	Aceptada
Usuario 8	Aceptada	Aceptada
Usuario 9	Aceptada	Aceptada
Usuario 10	No procesada	Aceptada
Usuario 11	Aceptada	Aceptada
Usuario 12	Aceptada	No Identificada
Usuario 13	Aceptada	Aceptada

Usuario 14	Aceptada	Aceptada
Usuario 15	Aceptada	Aceptada
Usuario 16	Aceptada	Aceptada
Usuario 17	Aceptada	Aceptada
Usuario 18	Aceptada	Aceptada
Usuario 19	Aceptada	Aceptada
Usuario 20	Aceptada	No Identificada
Usuario 21	Aceptada	Aceptada
Usuario 22	No procesada	Aceptada
Usuario 23	Aceptada	Aceptada
Usuario 24	Aceptada	Aceptada
Usuario 25	Aceptada	Aceptada
Usuario 26	Aceptada	Aceptada
Usuario 27	Aceptada	Aceptada
Usuario 28	Aceptada	No Identificada
Usuario 29	Aceptada	Aceptada
Usuario 30	Aceptada	Aceptada
Usuario 31	Aceptada	Aceptada
Usuario 32	Aceptada	Aceptada
Usuario 33	Aceptada	Aceptada
Usuario 34	Aceptada	Aceptada
Usuario 35	Aceptada	Aceptada

Usuario 36	Aceptada	Aceptada
Usuario 37	Aceptada	No Identificada
Usuario 38	Aceptada	Aceptada
Usuario 39	Aceptada	Aceptada
Usuario 40	Aceptada	Aceptada
Usuario 41	Aceptada	Aceptada
Usuario 42	Aceptada	Aceptada
Usuario 43	Aceptada	Aceptada
Usuario 44	Aceptada	Aceptada
Usuario 45	Aceptada	Aceptada
Usuario 46	Aceptada	Aceptada
Usuario 47	Aceptada	Aceptada
Usuario 48	Aceptada	No Identificada
Usuario 49	Aceptada	Aceptada
Usuario 50	Aceptada	Aceptada

Considerando las 98 huellas que fueron procesadas correctamente se obtuvieron los siguientes resultados:

FAR= (falsas aceptaciones/total de huellas procesadas)*100%

FAR=(0/98)*100%=0%

FRR= (falsos rechazos/total de huellas procesadas)*100%

FRR= (6/98)*100%=6.12%

La Tasa de validación de la huella dactilar se puede apreciar en la Figura 3.9.

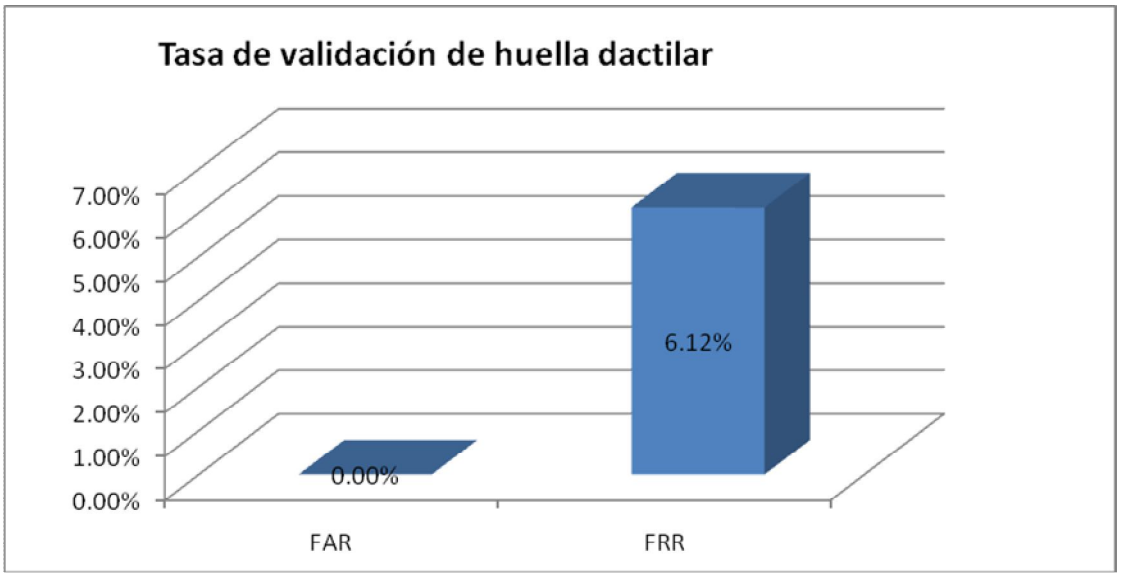


Figura 3.9: Tasa de validación de huella dactilar

Los resultados presentados son buenos, ya que los valores de la Tasa de Falsas Aceptaciones es realmente nulo, lo cual significa que al Sistema no puede ingresar una huella dactilar que no ha sido registrada, mientras que la Tasa de Falsos Rechazos es un valor realmente muy bajo, indicando que una mínima cantidad de huellas procesadas son rechazadas, de estos resultados se puede concluir que el sistema es confiable en la identificación de las huellas dactilares.

Otra forma de evaluación de los resultados del sistema, consiste en la aplicación de los Test de aceptación y Test de eficiencia.

El Test de aceptación es una técnica para medir diversos factores de la relación usuario-sistema, tales como la adaptabilidad, rapidez del aprendizaje, aceptación del diseño y nivel de integración del usuario con las operaciones del sistema. Es decir, el Test de aceptación se realiza para revelar que tan complacido está el usuario con el resultado final de la aplicación. La manera más eficiente de realizar este Test es realizando entrevistas a los usuarios que estén interactuando con el sistema, para de esta forma saber si la aplicación

contiene algún fallo, y de ser así que tan significante es dicho fallo. En nuestro caso se les aplica este Test a los trabajadores.

El Test de eficiencia es un instrumento aplicado en un equipo de trabajo o cliente, que busca determinar factores que indiquen el nivel de eficiencia del software basados en factores como funcionalidad, utilidad y mantenibilidad. En nuestro caso este Test se aplica a los directivos y funcionarios que controlan la asistencia mediante el sistema y emplean los diferentes tipos que reportes que se demandan.

Como parte de la evaluación de los resultados podemos plantear además las siguientes consideraciones:

- Un software de este tipo (similar) tiene un costo de 3500.00 USD en el mercado internacional.

- El incremento de la confiabilidad de la asistencia y permanencia del personal en las entidades de ETECSA, así como el control de los directivos hacia los trabajadores, redundan en un incremento de la eficiencia de la empresa y la productividad del trabajo.

- El ahorro de material de oficina que se empleaba es el siguiente:

Cantidad de trabajadores: 190

Cantidad de Libros de firma: 7

Cantidad de hojas mensuales: 30*7=210

Cantidad de hojas anuales: 210*12= 2520 (5 paquetes de hojas)

Cantidad de tóner anuales: 7

Cantidad de bolígrafos anuales: 7*6 (1 bolígrafo cada 2 meses)= 42

Costo de un paquete de hojas: 19.60 CUC

Costo de un tóner: 29.80 CUC

Costo de un bolígrafo: 0.98 CUC

Ahorro total anual por concepto de material de oficina: 347.76 CUC (este valor se incrementa en la medida que se extienda esta solución al resto de las entidades de ETECSA).

3.3. Reportes generados

En el software se incluye un módulo de reportes que brinda información a la gerencia de la empresa necesaria para su gestión.

3.3.1. Reporte de asistencias por día

El sistema brinda un reporte de la asistencia de todos los trabajadores para un día seleccionado, especificando para cada trabajador Nombre y Apellidos, Carne de Identidad, Departamento, Hora de llegada, Hora de salida y Cantidad de Horas trabajadas (Figura 3.10).

CI	Nombre y Apellidos	Departamento	Hora de llegada	Hora de salida	Cantidad de horas
77022149322	Odalys Martínez Marrero	Servicios Moviles	09:09	10:34	1.41
74021583345	Maidelys RodrÃguez DÃaz	Servicios Moviles	10:34	11:49	1.24
78060627809	Aned Cue Cabrera	Servicios Moviles	10:35	11:49	1.24
75110805501	Jorge Francisco Caraballo Rios	Capital Humano	09:09	10:34	1.42

Figura 3.10: Reporte de asistencias por día

3.3.2. Reporte de trabajadores ausentes por día

En la Figura 3.11 se muestra el reporte de todos los trabajadores ausentes para un día seleccionado, especificando para cada trabajador Nombre y Apellidos, Carne de Identidad y Departamento.

Figura 3.11: Reporte de trabajadores ausentes por día

3.3.3. Reporte de tardanzas por día

Un ejemplo de reporte relacionado con las llegadas tardes de los trabajadores se muestra en la Figura 3.12 donde se relacionan los trabajadores que tuvieron tardanza para un día seleccionado (llegada después de las 8:00 H), especificando para cada trabajador Nombre y Apellidos, Carne de Identidad, Departamento, Hora de llegada, Hora de salida y Cantidad de horas trabajadas.

CI	Nombre y Apellidos	Departamento	Hora de llegada	Hora de salida	Cantidad de horas
77022149322	Odalys Martínez Marrero	Servicios Moviles	08:53	13:43	4.84
74021583345	Maidelys RodrÃguez DÃaz	Servicios Moviles	08:53	14:04	5.18
78060627809	Aned Cue Cabrera	Servicios Moviles	08:54	14:18	5.4
75110805501	Jorge Francisco Caraballo Rios	Capital Humano	08:52	08:54	0.04
74100316602	Jennie HernÃ¡ndez RodrÃguez	Capital Humano	08:54	14:33	5.65
72051150156	JosÃ© Anselmo Ja MartÃnez	Capital Humano	08:55	14:34	5.65
76032294120	Nestor Alberto Lopez Romero	Capital Humano	08:55	14:34	5.65
72072338736	Nardys Valdes Fiffe	Capital Humano	08:56	14:35	5.65
78092227766	Maidalys Varela Delgado	Operaciones	08:57	14:35	5.64

Figura 3.12: Reporte de tardanzas por día

3.3.4. Reporte de asistencias por semana

Se visualiza en la Figura 3.13 el Reporte de asistencia de todos los trabajadores por semana, especificando para cada trabajador Nombre y Apellidos, Hora de llegada (en rojo si llega tarde, después de las 8:00 H) y Hora de salida (en azul si se va temprano, antes de las 17:30 H).

	15			16			17			18			19			20	
Nombre y Apellidos	I	F	H	I	F	H	I	F	H	I	F	H	I	F	H	I	F
Jorge Francisco Caraballo Rios	--:--	--:--	0	--:--	--:--	0	09:09	10:34	1.42	08:52	08:54	0.04	--:--	--:--	0	13:19	--:--
Odalys Martínez Marrero	--:--	--:--	0	--:--	--:--	0	09:09	10:34	1.41	08:53	13:43	4.84	--:--	--:--	0	--:--	--:--
Maidelys RodrÃguez DÃaz	--:--	--:--	0	--:--	--:--	0	10:34	11:49	1.24	08:53	14:04	5.18	--:--	--:--	0	--:--	--:--
Aned Cue Cabrera	--:--	--:--	0	--:--	--:--	0	10:35	11:49	1.24	08:54	14:18	5.4	--:--	--:--	0	--:--	--:--
Jennie HernÃjndez RodrÃguez	--:--	--:--	0	--:--	--:--	0	--:--	--:--	0	08:54	14:33	5.65	--:--	--:--	0	--:--	--:--
JosÃ© Anselmo Ja MartÃnez	--:--	--:--	0	--:--	--:--	0	--:--	--:--	0	08:55	14:34	5.65	--:--	--:--	0	--:--	--:--
Nestor Alberto Lopez Romero	--:--	--:--	0	--:--	--:--	0	--:--	--:--	0	08:55	14:34	5.65	--:--	--:--	0	--:--	--:--
Nardys Valdes Fiffe	--:--	--:--	0	--:--	--:--	0	--:--	--:--	0	08:56	14:35	5.65	--:--	--:--	0	--:--	--:--
Maidalys Varela Delgado	--:--	--:--	0	--:--	--:--	0	--:--	--:--	0	08:57	14:35	5.64	--:--	--:--	0	--:--	--:--

Figura 3.13: Reporte de asistencias por semana

3.3.5. Reporte de asistencias por trabajador en un periodo de tiempo

Se visualiza en la Figura 3.14 el Reporte de la asistencia de un trabajador para un período de tiempo seleccionado, especificando para cada trabajador Nombre y Apellidos, Carne de Identidad, Día, Hora de llegada y Hora de salida.

Figura 3.14: Reporte de asistencias por trabajador por periodo.

3.3.6. Reporte de ausencias por trabajador en un periodo de tiempo

Se visualiza en la Figura 3.15 el Reporte de las ausencias de un trabajador para un período de tiempo seleccionado, especificando para cada trabajador Nombre y Apellidos, Carne de Identidad, Día y estado (ausente).

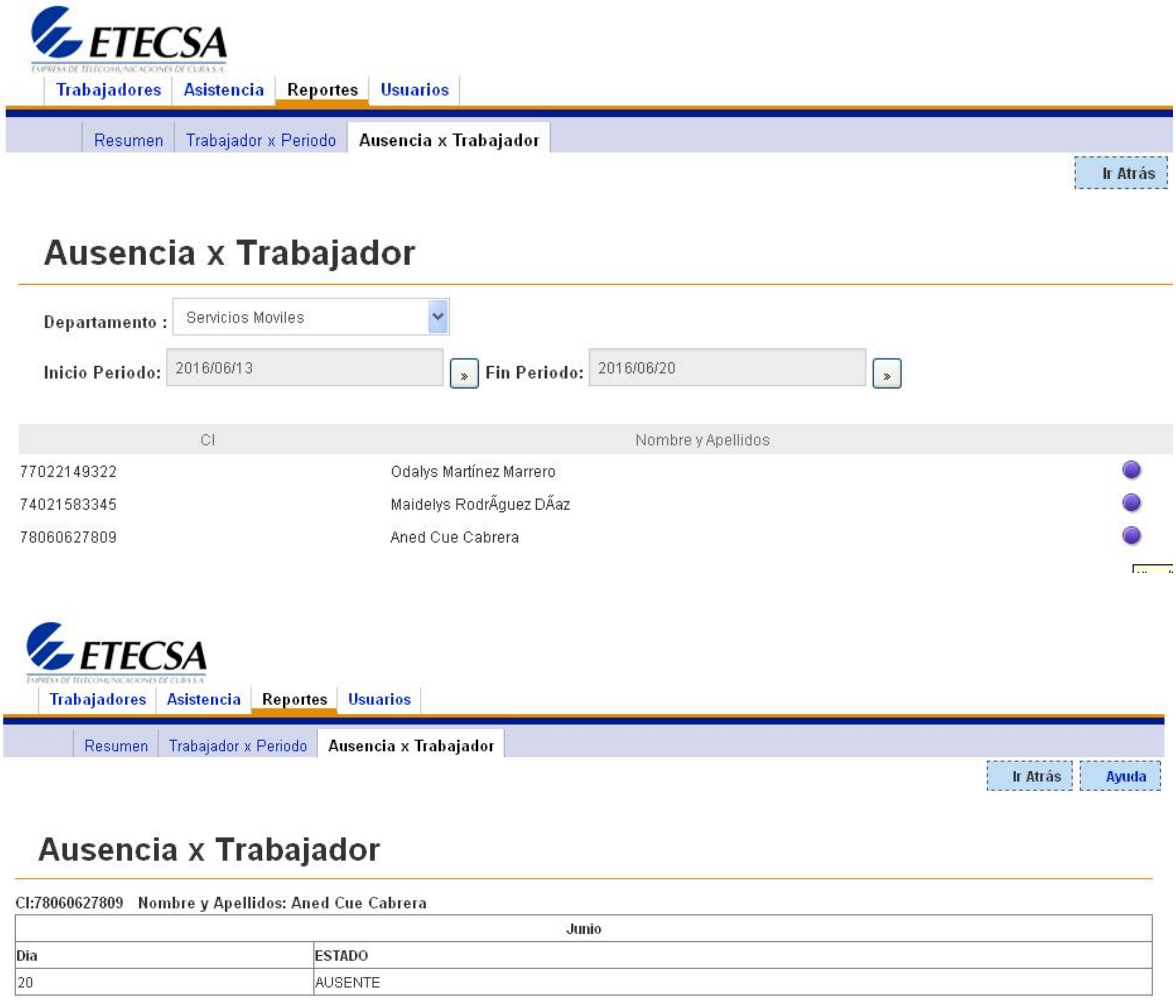


Figura 3.15: Reporte de ausencias por trabajador por periodo.

3.4. Consideraciones finales del capítulo

El funcionamiento del sistema biométrico propuesto para el control de asistencia de personal cumple con los procesos de registro y verificación de la huella dactilar, y en la evaluación de los resultados resulta un sistema confiable, efectivo, generalizable y de un ahorro económico muy importante. Los reportes generados por la aplicación le permiten a la administración lograr un adecuado control de la permanencia de sus empleados, lo que redunda en resultados positivos para la empresa.

Conclusiones

Como resultado de la investigación realizada se concluye que:

1. Los sistemas biométricos para el control de asistencia empleando diversas tecnologías, y específicamente los basados en huella dactilar, ofrecen una solución eficiente y confiable a los directivos de las empresas y entidades de Cuba y el mundo.
2. Se ha propuesto un sistema biométrico basado en huella dactilar económico, de fácil implementación y de gran importancia y utilidad, para el control de asistencia de los empleados de la Empresa de Telecomunicaciones de Cuba, especificando los elementos de hardware y software que los componen.
3. Con este trabajo se obtienen un conjunto de reportes que permiten a los directivos una adecuada gestión del capital humano y una mayor confiabilidad en los sistemas de pago.
4. Con el diseño del software para el control de asistencia se elimina un costo adicional en el proyecto, asi como el mismo se adapta a los requerimientos de la entidad.
5. Este proyecto forma parte de la realización de una Gestión Integral del Medio Ambiente y de lograr una producción mas limpia, al eliminar el consumo de hojas, toner y bolígrafos que por este concepto se emplean en la Empresa de Telecomunicaciones de Cuba, constituyendo un ahorro importante de estos recursos.

Recomendaciones

Como resultado de la investigación realizada se recomienda:

1. Aplicar esta solución a todas las dependencias del país de la Empresa de Telecomunicaciones de Cuba y hacia otras entidades de Cuba cuya relación costo-beneficio lo requieran.
2. Esta aplicación tiene la potencialidad de vincularse con el Sistema de Nómina de la empresa ETECSA, por lo que se recomienda su aplicación en este sentido, de forma tal que el pago a los trabajadores se genere de forma automática.

Referencias bibliográficas

[1] M. AG, «Donbass Arena Modern Video System Provides Security,» Mobotix AG, 28 Junio 2014. [En línea]. Available: http://www.mobotix.com. [Último acceso: 5 Julio 2016].

[2] Umanick, «Tecnologías Biométricas,» Umanick, 27 Junio 2012. [En línea]. Available: http//www.umanick.com. [Último acceso: 10 Junio 2016].

[3] X. Biometrics, «Proyecto ISIS International Soccer Identification System,» Xelios Biometrics, 30 Junio 2012. [En línea]. Available: http://www.xelios.es. [Último acceso: 15 Julio 2016].

[4] «Futronic_Finger,» Futronic_Finger, 30 Septiembre 2012. [En línea]. Available: http:/article.wn.com. [Último acceso: 16 Julio 2016].

[5] M. SAP, «Aplicaciones Biométricas,» Mercurio SAP, 2 Julio 2013. [En línea]. Available: http://www.edicionesespeciales.elmercurio.com. [Último acceso: 26 Junio 2016].

[6] Jain, «Intelligent Biometric Techniques in Fingerprint and Face Recognition,» Jain, 12 Diciembre 2012. [En línea]. Available: http://bias.csr.unibo.it. [Último acceso: 13 Julio 2016].

[7] A. Czajka, «Template Ageing in Iris Recognition,» vol. 1, nº 2, 15 Mayo 2013.

[8] C. H. a. R. M. Garces, «Análisis de un sistema de autenticación por huella dactilar para fortalecer el sistema de seguridad para utilizar el software de la Empresa Farmacéuticos,» de Teoría general de los sistemas volumen 1, Venezuela, Nueva Línea, 2013.

[9] A. U. a. I. University, «Biometric Acces Control System Using Automared Recognition,» Air University and Iqra University, 24 Julio 2014. [En línea]. Available: http://iqrauniversity.edu.pk. [Último acceso: 10 Julio 2016].

[10] U. C. I. d. Madrid, «Privacy And Legal Requirement for Developing Biometric Identification Software in Context-Based Aplications,» Universidad Carlos III de Madrid, 20 Diciembre 2010. [En línea]. Available: http://www.serc.org. [Último acceso: 14 Julio 2016].

[11] C. I. o. T. o. Kokrajhar, «Interner Banking Risk Analysis And Applicability of Biometric Technology for Authentication,» Central Institute of Technology of Kokrajhar, 13 Agosto 2013. [En línea]. Available: http://www.serc.org. [Último acceso: 10 Junio 2016].

[12] G. Herbert, «Biometria y la aplicacion de personas,» Gutierrez Herbert, 20 Noviembre 2007. [En línea]. Available: http://capacitacionencostos.blogia.com. [Último acceso: 5 Julio 2016].

[13] E. Amable, «Tecnologías de Identificación,» Edgardo Amable, 20 Septiembre 2007. [En línea]. Available: http://www.geocities.com. [Último acceso: 24 Mayo 2016].

[14] C. Belloch, «Entornos visuales de formacion,» C. Belloch, 23 Diciembre 2012. [En línea]. Available: http://www.uv.es/bellochc/pedagogia/EVA9.wiki?3. [Último acceso: 30 Julio 2016].

[15] M. Aguilera, «Reconocimiento biométrico basado en huellas palmares,» Universidad autonoma de Madrid, 20 Diciembre 2012. [En línea]. Available: http://www.biometria.gov.ar. [Último acceso: 13 Junio 2016].

[16] Amazon, «Books Automatic Fingerprint Recognition Systema,» Amazon, 22 Diciembre 2013. [En línea]. Available: http://www.amazon.com. [Último acceso: 14 Junio 2016].

[17] INTECO, Estudio sobre las tecnologías biométricas aplicadas a la Seguridad, vol. 1, Madrid: INTECO, 2011.

[18] I. E. d. E. S. Madrid, Tecnologías Biométricas y sus aplicaciones, vol. 1, Madrid: Instituto Especializado de Estudios Superiores Madrid, 2014.

[19] J. Costas Santos, Sistemas Biométricos, vol. 2, Madrid: JC.RA, 2011.

[20] Accesor, «Sistemas Biométricos: Matching de huellas dactilares mediante transformada de Hougg generalizada,» Accesor, 26 Abril 2014. [En línea]. Available: http://www2.ing.puc.cl. [Último acceso: 18 Junio 2016].

[21] V. Matyas, Biometric Authentication, Security and Usability, vol. 1, Londres: Riha, 2012.

[22] F. N. Teccnologies, «Feedback Networks,» Networks Teccnologies, 8 Abril 2014. [En línea]. Available: http://feedbacknetworks.com. [Último acceso: 25 Julio 2016].

[23] C. d. I. Loyola, Proyectos de Biometría, vol. 1, Republica Dominicana: IEESL, 2013.

[24] H. Briones, Red y seguridad biométrica, vol. 1, Mexico: UNAM, 2014.

[25] A. Gualberto, Reconocimiento de huellas dactilares usando caracteristicas locales, vol. 1, Mexico: GSMexico, 2014.

[26] U. P. d. Madrid, Las Tecnologías Biométricas aplicadas a la seguridad, vol. 2, Madrid: INTECO, 2013.

[27] N. S., Seguridad fisica en instalaciones criticas, vol. 2, Madrid: APC, 2013.

[28] J. G, Tu huella en la entrada al smartphone, vol. 2, Madrid: UNO, 2013.

[29] I. B. Group, «Comparative Biometric Testing,» International Biometric Group, 23 Octubre 2014. [En línea]. Available: http://www.ibgweb.com. [Último acceso: 14 Julio 2016].

[30] Bioidentidad, Biosuprema BioEntryPlus, vol. 1, Londres: Bioidentidad, 2014.

[31] I. E. d. E. S. LOYOLA, «Sensores Biométricos,» Instituto Especializado de Estudios Superiones LOYOLA, 5 Febrero 2014. [En línea]. Available: http://superior.ipl.edu.do. [Último acceso: 6 Julio 2016].

[32] O. d. l. S. d. l. Informacion, «Sensores Biometricos,» INTECO, 23 Septiembre 2014. [En línea]. Available: http://www.europeanbiometrics.info. [Último acceso: 21 Julio 2016].

[33] S. Corporation, SecuGen USB Fingerprint Reader User Guide, vol. 1, Londres: SecuGen Corporation, 2013.

[34] Kimaldi, Lectores de huella digital, vol. 1, Madrid: Kimaldi, 2013.

[35] J. Ortega, «Info Biometric,» INTECO, 22 Septiembre 2014. [En línea]. Available: http://www.infosyssec.net. [Último acceso: 23 Junio 2016].

[36] EVA, «EVA Manuales,» EVA Manuales, 26 Marzo 2014. [En línea]. Available: http://www.php.net. [Último acceso: 21 Julio 2016].

[37] J. flash, «Soluciones CIC,» Java flash, 12 Abril 2013. [En línea]. Available: http://www.cic.com. [Último acceso: 30 Junio 2016].

[38] B. Group, «Biometric Software,» Biometric Group, 28 Noviembre 2014. [En línea]. Available: http://www.biometricgroup.com. [Último acceso: 1 Julio 2016].

[39] G. A. v.Graevenitz, «System evaluations Biometric Finger,» Applied Biometrics GmbH, 22 Noviembre 2014. [En línea]. Available: http://www.atmmarketplace.com. [Último acceso: 12 Julio 2016].

Anexos

Anexo I Errores en los sistemas biométricos

La salida resultante del módulo de coincidencia en un sistema de reconocimiento basado en huellas dactilares, típicamente es una puntuación que cuantifica el grado de similitud entre la plantilla de entrada y la plantilla almacenada en la base de datos, y puede ser considerada sin pérdida de generalidad dentro del rango de cero a uno. Una puntuación cercana a uno, indica una alta certeza de que las dos impresiones provengan de la misma huella, en caso de que la puntuación este cercana a cero, indica una baja certeza de que las dos impresiones provengan de la misma huella. La decisión del sistema está regulada por un valor umbral **t,** los pares que generan puntuaciones mayores o iguales que **t**, se deduce que son "pares de coincidencia" (es decir, pertenecen a la misma huella), y los pares que generan puntuaciones menores que **t** se deduce que son "pares de no coincidencia" (es decir, que pertenecen a diferentes huellas.)

Desde el punto de vista del diseño, el problema de la verificación biométrica puede ser formulado de la siguiente manera:

Sea **Ts** la plantilla de impresión dactilar almacenada en la base de datos (conocida también con el nombre de impresión secundaria) y **Tp** la plantilla de impresión dactilar adquirida para la verificación (conocida como impresión dactilar primaria). Entonces las hipótesis que pueden ser definidas son:

HO: Tp<>Ts – La impresión dactilar primaria no es la misma que la impresión dactilar secundaria

H1: Tp = Ts – La impresión dactilar primaria es la misma que la impresión dactilar secundaria.

Las decisiones asociadas con cada una de las hipótesis son:

D0: El individuo es un impostor

D1: El individuo es quien dice ser

En la siguiente Figura A1.1 se muestran los errores en el reconocimiento positivo y negativo de un sistema biométrico.

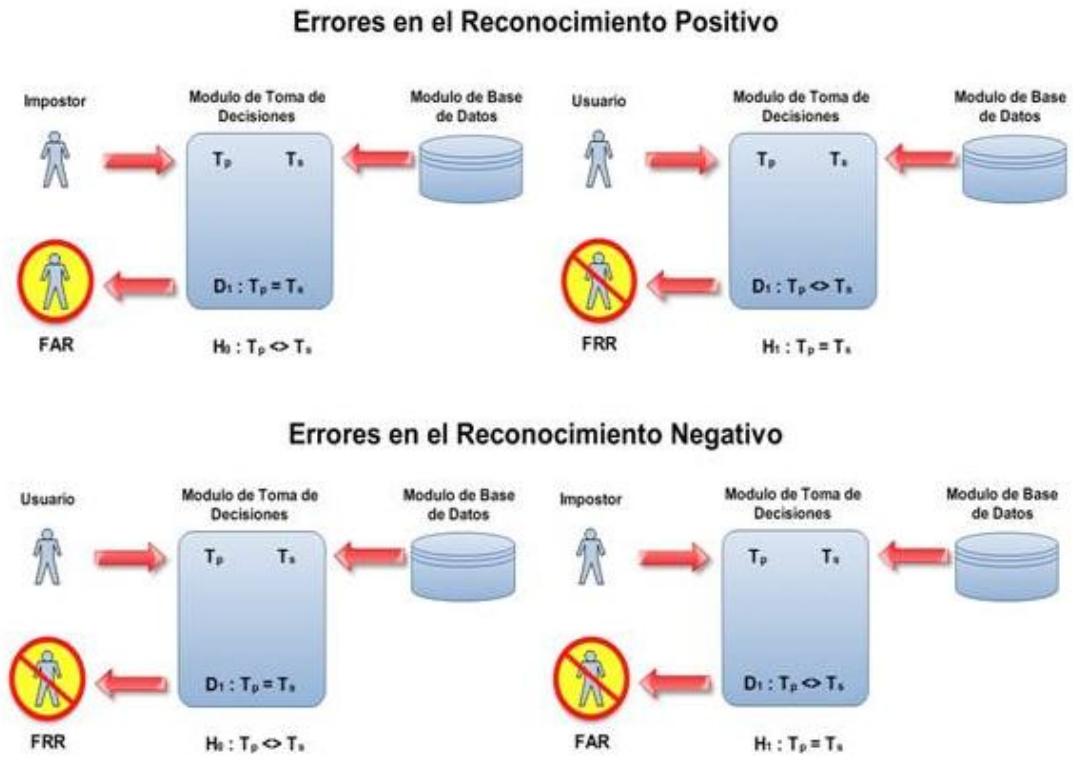


Figura A1.1: Errores en el reconocimiento positivo y negativo

Anexo II Algunos dispositivos (relojes) biométricos de control de asistencia

A continuación presentaremos algunos dispositivos (relojes) biométricos de control de asistencia Murdoch, empresa peruana dedicada a la comercialización de equipos para sistemas de identificación y control de asistencia, entre otros:

- Reloj Biométrico H3: Reloj de control de asistencia con lector de huella digital. Puerto USB para conexión directa con su computadora y pantalla LCD monocromática. Almacena aproximadamente 30,000 registros. Reloj de escritorio para control de personal, orientado a oficinas con pocos trabajadores. Estructura blanca de moderno diseño. En la Figura A2.1 se muestra este reloj biométrico.

Figura A2.1: Reloj Biométrico H3

- Reloj Biométrico H5: Cuenta con lector de huella digital (biométrico), puerto USB para conexión directa con la computadora y pantalla a color TFT de 3".Almacena aproximadamente 30,000 registros. Es un reloj de escritorio para control de personal, orientado a oficinas con pocos trabajadores. Estructura de moderno diseño. En la Figura A2.2 se observa este reloj biométrico.

Figura A2.2: Reloj Biométrico H5

- Reloj Biométrico IN01-A: Cuenta con lector de huella digital y opcionalmente, tarjeta de proximidad. Cuenta con puerto USB para conexión directa con la computadora y pantalla a color de 3". Almacena aproximadamente 30,000 registros. Cuenta con batería interna de aprox. 3 horas para asegurar el funcionamiento en caso de pérdida de alimentación. En la Figura siguiente A2.3 se puede apreciar este reloj biométrico.

Figura A2.3: Reloj Biométrico IN01-A

- Reloj Biométrico X628-C: Equipo ideal para toda institución, elimina el control con fotocheck. Marcación de asistencia precisa y rápida, se conecta y listo para funcionar. Lector de huella digital, con capacidad de 3,000 imágenes de huellas digitales utilizando un número de identificación. Comunicación TCP/IP (red), vía RS-232 (serial), USB. No esclaviza a una computadora. Tiempo de verificación de huella de 1.5 segundos. Memoria para 50,000 marcaciones de asistencia antes de

descargar a una computadora. El Reloj Biométrico X628-C se puede apreciar en la siguiente Figura A2.4.

Figura A2.4: Reloj Biométrico X628-C

- Reloj Biométrico iClock 360: Cuenta con lector de huella digital para registrar la asistencia. Capacidad de 10,000 imágenes de huellas digitales y 200,000 marcaciones. Incorpora puerto USB para descarga de marcaciones. Trabaja en red protocolo TCP/IP. Comunicación vía RS-232 o TCP/IP (red). Tiempo de verificación de huella de 1.5 segundos. Memoria RAM de 512 Kb. para 200,000 marcaciones de asistencia. Pantalla LCD (TFT) Multimedia iluminada. Lector de tarjetas de proximidad. En la Figura siguiente A2.5 se puede apreciar este reloj biométrico.

Figura A2.5: Reloj Biométrico iClock 360

- Reloj Biométrico iClock 580: Distintos modos de operación: sólo huella, clave, huella y clave y tarjetas de proximidad. Incorpora puerto USB para descarga de fichajes o para comunicación con una computadora. 50 zonas horarias y 5 grupos de acceso. Relé para apertura de puerta, alarma. Los terminales iClock 580 son equipos de Control de Asistencia y/o Accesos que permiten trabajar en modo autónomo (sin una computadora) o integrarse fácilmente a una aplicación de Control de Asistencia y/o accesos mediante comunicación USB o Ethernet (red TCP/IP). El reloj biométrico iClock 580 se muestra a continuación en la Figura A2.6.

Figura A2.6: Reloj Biométrico iClock580

- Reloj Biométrico iClock 660: Display color TFT de 3,5". Pantalla LCD (TFT) Multimedia iluminada. Cámara integrada. Distintos modos de operación: sólo Huella y Huella + PIN. Opcionalmente: Huella + Tarjeta y Tarjeta + PIN. Incorpora puerto USB para descarga de marcaciones. Capacidad: Hasta: 60,000 usuarios. Memoria RAM de 512 Kb. para 200,000 marcaciones. En la Figura siguiente A2.7 se puede apreciar este reloj biométrico.

Figura A2.7: Reloj Biométrico iClock660

- Reloj Biométrico doble DS100-ID: Reloj biométrico innovación en el control de asistencias del personal con tecnología de doble huella digital. Permite almacenar hasta 100000 eventos y 6000 huellas. Esta información puede ser descargada a través de la red o por una memoria USB o tarjeta SD. Cuenta con una pantalla TFT de 3 pulgadas. Es ideal para pequeñas, medianas y grandes empresas. En la Figura A2.8 se puede observar este reloj biométrico.

Figura A2.8: Reloj Biométrico doble DS100-ID

- Reloj Biométrico facial iFace 402: Reloj multimedia de última generación con reconocimiento facial para registrar asistencia. Modos de operación: Reconocimiento facial, huella dactilar, tarjeta de proximidad y password. Pantalla táctil TFT de 4.3’’. Manejo sencillo y moderna interface. Cámara integrada. Sistema óptico de infrarrojos para identificación del usuario en ambientes oscuros. Puerto

USB para descarga de fichajes. Trabaja en red protocolo TCP/IP. Muestra en pantalla datos del trabajador que registra asistencia. En la Figura A2.9 se puede observar este reloj biométrico.

Figura A2.9: Reloj Biométrico facial iFace 402

Anexo III Forma correcta de ubicar el dedo sobre el escáner

En la Figura A3.1 se muestra la forma correcta de ubicar el dedo en el escáner.

Figura A3.1: Forma correcta de ubicar el dedo sobre el escáner