Universidad de las Ciencias Informáticas

Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas

Componente para la Comparación de Huellas Dactilares en Tarjetas Inteligentes

Autores

Abel Ernesto Sánchez Alí

Raúl Angel Ballester Mena

Tutores

Ing. Yerandy Arias González

Ing. Rafael Leodan Cardero Álvarez

Ciudad de La Habana, Junio 2010

"Año 52 de la Revolución"

DECLARACIÓN DE AUTORÍA

Nosotros: **Raúl Angel Ballester Mena y Abel Ernesto Sánchez Alí**, nos declaramos como únicos autores del presente trabajo y autorizamos a la Universidad de las Ciencias Informáticas (UCI) a que haga uso del mismo de la manera que mejor estime. Y para que así conste firmamos la presente a los __ días del mes de _____de 2010.

_____ _____

Raúl Angel Ballester Mena Abel Ernesto Sánchez Alí

_____ _____

Ing. Yerandy Arias González Ing. Rafael Leodan Cardero Álvarez

DATOS DE CONTACTO

Ing. Yerandy Arias González: Profesor graduado de Ingeniería en Ciencias Informáticas. Se desempeña como jefe del proyecto de huellas dactilares en el Centro de Identificación y Seguridad Digital. Ha participado en eventos científicos como UCIENCIA, RECPAT, Fórum de Ciencia y Técnica y fue seleccionado como mención al premio CITMA en el curso 2008-2009.

Ing. Rafael Leodan Cardero Álvarez: Profesor graduado de Ingeniería en Ciencias Informáticas. Se ha desempeñado como jefe de departamento en el Centro "Informática médica". Actualmente es asesor de investigación en el departamento "Señales digitales", perteneciente al Centro "Geoinformática y señales digitales". Las áreas de investigación de interés son la Visión artificial, el análisis de imágenes de documentos (DIA) y la administración de industrias de la información. Ha recibido 11 cursos de postgrado y ha estado relacionado con la impartición de 2 cursos de postgrado. Ha presentado artículos en eventos como la Conferencia Científica UCIENCIA y el Congreso Nacional de Reconocimiento de Patrones. Tiene un artículo aceptado y pendiente de publicación en la Revista Ciencias de la Información.

AGRADECIMIENTOS

A mis amigos Mok, Gerardo, Javier, Osmel, Merayo, Gustavo, Ernesto, Adalberto, Aliet, Yamacho, Luis, Adrian, Boloy, Manuel, Carlos, Marlon y a todos los demás, por estar siempre conmigo en los mejores y en los peores momentos de la vida

A mis compañeros del apartamento, por ser mis amigos y poder contar con cada uno de ellos.

A mis tutores, un verdadero tutor es un verdadero amigo: muchas gracias

A mis tíos, por ser mis padres también y contar siempre con ellos

A mis abuelos, por quererme tanto y trasmitirme sus experiencias

A Abel, por ser más que un compañero de tesis y más que un amigo, mi hermano

A todos los que me ayudaron en el desarrollo del trabajo de diploma y de forma especial a toda mi familia

Ballester

A la gente del 2 por pasar junto conmigo esos momentos.

A la gente de los acostumbrados debates por querer arreglar el mundo.

A Baller por ser mi hermano y aportar leyes muy útiles.

A Leidys y Bety por ayudar y criticar tanto este documento.

A todos los que compartimos en este tiempo de tesis, los "best", a los del Karaoke.

A mis tutores y oponente por la manera particular de ayudarme.

A Teufel, DKey y al Matatán, por ser tan especiales.

Y a Moni porque si.

Abel

DEDICATORIA

A mis padres, por su confianza, por ser mis guías y quererme tanto (...)

A mi hermana, por ser tan linda y ocuparse siempre de mí

A mi novia por estar siempre para apoyarme y compartir su vida conmigo

A mi hijo, por ser la alegría de mi vida.

Ballester

A Mami por estar siempre a mi lado y ser esa mujer excepcional de la que estoy muy orgulloso.

A Papi por ser quien me enseño la curiosidad por saber desde muy pequeño y por ser el.

A la mia Gioia por compartir conmigo un millón de sueños.

A mi Familia que siempre me sigue, me apoya y espera lo mejor de mí en cada momento.

Abel

RESUMEN

El uso de las huellas dactilares es una de las formas de identificación biométrica más antiguas y más utilizadas. Las nuevas aplicaciones sobre tarjetas inteligentes permiten incluir sistemas biométricos que cuentan con un componente de comparación para verificar la identidad del titular de la tarjeta. El Centro de Identidad y Seguridad Digital está involucrado en el despliegue de millones de cédulas de identificación sobre tarjetas. Por lo que es de vital importancia el desarrollo de un componente de comparación para estas cédulas.

En el presente trabajo de diploma se definió como objetivo del trabajo desarrollar un componente para la comparación de huellas dactilares en tarjetas inteligentes. Se muestra un análisis del las tendencias de la comparación de huellas dactilares, un estudio de las características particulares de los componentes biométricos en tarjetas inteligentes y los estándares del mercado aplicados a estas tecnologías.

Se diseña e implementa el componente usando la tendencia basada en minucias sobre el lenguaje C y haciendo uso de las metodologías de desarrollo Scrum y XP. Al mismo se le realizaron pruebas usando una porción de la base de datos de ciudadanos obteniéndose resultados satisfactorios.

Este componente le permitirá al país ahorrar divisa por concepto de importación de software. Es un importante hito tecnológico pues es el primer MoC que se registra en Cuba y además sienta las bases para la creación de un futuro sistema AFIS.

INDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

LISTA DE ACRÓNIMOS

AFIS	*Automated Fingerprint Identification System*. Sistema de Identificación Automática de Huellas Dactilares.
API	*Application Programming Interface*. Interfaz de Programación de Aplicaciones.
CPU	*Central Processing Unit*. Unidad Central de Proceso.
EEPROM	*Electrically-Erasable Programmable Read-Only Memory*.
ERR	*Equal Error Rate*. Tasa de Igualdad de Error.
FAR	*False Acceptance Rate*. Tasa de Falsos Aceptados.
FRR	*False Rejection Rate.* Tasa de Falsos Rechazados.
GSM	*Groupe Special Mobile.* Sistema Global para las Comunicaciones Móviles.
IDE	*Integrated Development Environment.* Entorno de Desarrollo Integrado.
IEC	*International Electrotechnical Commission.* Comisión Electrotécnica Internacional.
INCITS	*InterNational Committee for Information Technology Standards.*
ISO	*International Organization for Standardization.*
JC	*Java Card.*
JVM	*Java Virtual Machine.* Máquina Virtual de Java.
MoC	*Match on Card.* Comparación en Tarjeta.
MS-DOS	*MicroSoft Disk Operating System.* Sistema operativo de disco de Microsoft.
NIST	*National Institute of Standards and Technology.* Instituto Nacional de Normas y Tecnología.
OS	*Operating System.* Sistema Operativo.
PIN	*Personal Identification Number.* Número de Identificación Personal.
PIV	*Personal Identity Verification.*
RAM	*Random Access Memory.* Memoria de Acceso Aleatorio.
ROM	*Read-Only Memory.* Memoria de Solo Lectura.
SIM	*Subscriber Identity Module.* Módulo de Identificación del suscriptor.
STEP	*Secure Trusted Environment Provisioning.*
TLV	*Type, Length and Value.* Tipo, Longitud y Valor.
UCI	Universidad de las Ciencias Informáticas.
UML	*Unified Modeling Language.* Lenguaje Unificado de Modelado.
XML	*Extensible Markup Language.* Lenguaje de marcas extensible.

XP	*Extreme Programming.* Programación Extrema.

INTRODUCCIÓN

Con la evolución de las tecnologías asociadas a la información, la sociedad está cada día más conectada electrónicamente. Labores que tradicionalmente eran realizadas por seres humanos son, gracias a las mejoras tecnológicas, realizadas por sistemas automatizados. Dentro de la amplia gama de posibles actividades que pueden automatizarse, aquella relacionada con la capacidad para establecer la identidad de los individuos ha cobrado importancia y como consecuencia directa la Biometría se ha transformado en un área emergente.

La Biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento. Una característica anatómica tiene la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano, patrones de la retina o el iris. Un rasgo del comportamiento es menos estable, pues depende de la disposición psicológica de la persona, por ejemplo la firma. No cualquier característica anatómica puede ser utilizada con éxito por un sistema biométrico. Para que esto así sea debe cumplir con las siguientes características: (1)

- *Universalidad*: Indica qué tan común es de encontrar entre los individuos.
- *Singularidad*: Indica con qué grado de diferencia existe entre de los individuos.
- *Permanencia*: Indica qué tanto perdura en el tiempo de manera inalterable.
- *Recolectable*: Indica su facilidad de adquisición, medición y almacenamiento.
- *Calidad*: Indica qué tan preciso, veloz y robusto es el sistema en su manejo.
- *Aceptabilidad*: Indica el grado de aprobación que tiene la tecnología entre el público.
- *Fiabilidad*: Indica la facilidad de engañar al sistema de autenticación.

Un indicador biométrico que satisface estos requisitos es la huella dactilar (**¡Error! No se encuentra el origen de la referencia.**), que ha sido utilizado por los seres humanos para la identificación de personas. En la actualidad la identificación mediante huellas dactilares representa una de las tecnologías biométricas más maduras y es considerada una prueba legítima de evidencia criminal en cualquier corte judicial del mundo.

Tabla 1 Comparación de Sistemas Biométricos

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Vascular dedo	Geometría de la mano	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Muy alta	Muy Alta	Muy alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Muy alta	Alta	Media	Media	Media
Aceptación	Media	Baja	Alta	Alta	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Media	Baja	Media	Media

Una huella dactilar (Figura 1) es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela. Sin embargo, estas líneas se interceptan y a veces terminan en forma abrupta. Los puntos donde estas terminan o se bifurcan son tipos de minucias o patrones específicos de esas líneas de la epidermis.

Para verificar si dos huellas dactilares corresponden o no a la misma persona se lleva a cabo un procedimiento que comienza con la clasificación de la huella dactilar y termina con la comparación de las minucias de ambas huellas. La clasificación de huellas corresponde a un análisis de los patrones globales de la huella que permite asignarla a un conjunto predeterminado o clase, lo que se traduce en una partición de la base de datos a ser revisada. Por otro lado, las huellas se comparan según sus características, ya sea por su apariencia, la forma de sus crestas o por la geometría de puntos característicos de estas. En otras palabras, la comparación de huellas dactilares consiste en encontrar el grado de similitud entre dos de ellas.

Figura 1. Huella dactilar.

Las principales dificultades en el proceso de comparación son:

- La huella tomada puede estar expuesta a transformaciones lineales como son de rotación o de traslación; o a cierta trasformación no lineal elástica producto de la proyección de una superficie tridimensional como el dedo en una superficie bidimensional, también acentuada por la presión con que se ejerció en la toma.
- La huella a comparar puede estar incompleta debido a que es dejada de forma accidental en algún escenario, lo que implica que no posee toda su información.
- Las condiciones de la toma, el método de adquisición, el sudor y otras condiciones influyen en la calidad de la huella obtenida, lo que produce zonas irreconocibles o introduce detalles indeseados.

Una de las referencias más antiguas del uso de la comparación de huellas se encuentra en el año 33 a.C[1], cuando Quintiliano, retórico y pedagogo hispanorromano escribió acerca de un ciego acusado de asesinato que justificó su inocencia por medio de las huellas que se encontraron en el lugar del crimen. Sin embargo, existen fuentes más antiguas que hablan del uso de esta ciencia en China en el siglo VII a.C. para sellar pactos comerciales. (2)

Se puede considerar que uno de los primeros hitos de esta ciencia es el inicio de los estudios del relieve de los dedos y las palmas de las manos en 1665 por Marcelo Malpighi, profesor de histología y anatomía. Malpighi está considerado como el primer estudioso de esta ciencia. Pero se necesitarían dos siglos para que el científico checo Juan Evangelista Purkinje implantara en 1823 un método científico para el estudio de los relieves de la epidermis. Otro de los principales hitos, podría considerarse el inicio de la aplicación de las técnicas existentes para la identificación de personas en 1858 por William James Herschel, gobernador en la India. Los motivos de Herschel no tenían mucho que ver con mejorar la situación social de sus trabajadores sino con evitar que los trabajadores utilizaran identidades diferentes. (3)

Actualmente en el mundo existen sistemas para controlar el acceso de personas a varias instituciones o locales, que se basan fundamentalmente su identificación en el uso de credenciales, tarjetas magnéticas o contraseñas. Aunque así lo parezca, estos métodos no son

[1] a.C. Antes de Cristo.

muy seguros, ya que objetos como tarjetas de acceso pueden ser compartidos o robados y no se puede diferenciar entre un usuario autorizado y otro que no lo esté. Esto es debido a que dichas credenciales no poseen ninguna información biométrica, facilitando así la violación de la seguridad.

La necesidad de que automáticamente se identifique a una persona es cada vez más frecuente. Por otro lado, las nuevas aplicaciones que están surgiendo sobre tarjetas inteligentes (Figura 2) permiten incluir sistemas biométricos. El componente para la comparación de los rasgos es la pieza principal para realizar la autenticación del titular de la tarjeta.

Figura 2. Tarjeta Inteligente.

Esta tecnología es relativamente joven, ya que las tarjetas fueron inventadas y patentadas en los setenta. Existen algunas discusiones de quién es el inventor original entre los que se encuentran: Juergen Dethloff de Alemania, Arimura de Japón y Roland Moreno de Francia. El primer uso masivo de las tarjetas fue para el pago telefónico público en Francia en 1983. Desde sus inicios en los años 70, la historia de tarjetas inteligentes ha reflejado los constantes avances en capacidades técnicas y ámbitos de aplicabilidad. (4)

El mayor auge de las tarjetas inteligentes fue en los noventa, con la introducción de las tarjetas SIM utilizadas en la telefonía móvil GSM en Europa. Aunque existían prototipos, no es hasta finales de esta década en 1999 que salen al mercado de forma masiva las tarjetas sin contactos, debido principalmente a los problemas para integrar la antena en la tarjeta. (5)

Surge entonces la necesidad de contar con un componente para la comparación de huellas dactilares sobre tarjetas inteligentes, con un alto grado de confiabilidad y que cumpla con los

estándares internacionales para estos sistemas, para brindarle al país una de las tecnologías más populares de identificación en la actualidad.

A partir de la situación descrita anteriormente se identifica el **problema científico** ¿Cómo comparar huellas dactilares en sistemas de tarjetas inteligentes? El problema científico delimita el **objeto de estudio** la verificación de identidad mediante la comparación de huellas dactilares. El objeto de estudio se enmarca en el **campo de acción.** Los procesos para la comparación de huellas dactilares en tarjetas inteligentes. Por lo antes planteado se definió como **objetivo del trabajo** desarrollar un componente para la comparación de huellas dactilares en tarjetas inteligentes. Para cumplir el objetivo propuesto se trazaron las siguientes **tareas de investigación**:

1. Investigar las tecnologías y los estándares de comparación de huellas dactilares en tarjetas inteligentes.
2. Analizar los algoritmos de comparación de huellas dactilares existentes.
3. Diseñar un algoritmo para la comparación de huellas en tarjetas inteligentes.
4. Implementar un algoritmo para la comparación de huellas en tarjetas inteligentes.
5. Obtener los indicadores de calidad del algoritmo implementado y compararlos con referencias mundiales.

CAPÍTULO 1 .FUNDAMENTACIÓN TEÓRICA

En este capítulo se abunda sobre el estado del arte del tema tratado a nivel internacional, nacional y de la universidad. Se describen las tecnologías, metodología y herramientas utilizadas para el desarrollo del componente.

1.1. Tarjetas inteligentes

Una tarjeta inteligente (Smart Card) es una tarjeta de plástico, de dimensiones normalizadas (las mismas que una tarjeta de crédito), que tiene empotrado en su interior un chip que le permite realizar cierta lógica programada. Además puede tener capacidad de almacenamiento.

1.1.1. Clasificaciones

Las tarjetas inteligentes se pueden clasificar según diversos criterios:

- Según la capacidad de su chip.
- Según la estructura de su sistema operativo.
- Según la interfaz de comunicación.

Tarjetas inteligentes según la capacidad de su chip

- *Memoria*: tarjetas que únicamente funcionan para el almacenamiento de datos. No son capaces de procesar información. Se usan generalmente en aplicaciones sin altos requisitos de seguridad.
- *Microprocesador*: tarjetas con una estructura análoga a la de una computadora (procesador, memoria volátil, memoria persistente). Contienen ficheros y aplicaciones que les permite implementar avanzados mecanismos de seguridad para proteger la información contenida en ellas. Suelen usarse en sistemas de identificación biométricos y sistemas de pago.
- *Criptográficas*: Tarjetas con microprocesador muy avanzadas que cuentan con un coprocesador criptográfico para la ejecución de algoritmos complejos usados para el cifrado de la información y la firma digital de documentos. Estas tarjetas pueden

almacenar de forma segura uno o varios certificados digitales y se pueden utilizar para firmar documentos o autenticar al titular de la misma sin que la información “sensible” contenida en su memoria salga de ella.

Tarjetas inteligentes según la estructura de su sistema operativo

- *Tarjetas de memoria*: disponen de un elemental sistema operativo limitado a una serie de comandos básicos de lectura y escritura de las distintas secciones de memoria y la protección de la información está condicionada a la presentación de un código secreto.
- *Tarjetas basadas en ficheros*: estas tarjetas disponen del equivalente a un sistema de ficheros MS-DOS con dos niveles de jerarquía. Hay directorios y ficheros. Tienen un sistema operativo con un conjunto de comandos que le ofrecen las operaciones básicas para el acceso a los datos y la protección de la información.
- *Tarjetas Java*: son capaces de ejecutar mini-aplicaciones Java. Su sistema operativo es una pequeña máquina virtual Java (JVM) y en ellas se pueden cargar dinámicamente aplicaciones desarrolladas específicamente para este entorno.

Tarjetas inteligentes según la interfaz de comunicación

- *Tarjetas de Contacto*: son las que necesitan ser insertadas en un lector de tarjetas para ser accedidas mediante los contactos físicos del chip.
- *Tarjetas sin Contacto*: son las que se comunican usando radio frecuencia. Para ser accedidas sólo se requiere la proximidad al lector. El chip se encuentra en la parte interna y está conectado a una antena que permite la comunicación con el lector.
- *Tarjetas Dual*: cuentan con un único chip que se comunica a través de dos interfaces: de contacto y sin contacto. Poseen las características de las mencionadas anteriormente.
- *Tarjetas Híbridas*: son aquellas que tienen dos chips independientes, cada uno con una interfaz diferente; uno con interfaz de contacto y otro con una interfaz sin contacto.

1.1.2. Estructura de una tarjeta inteligente

Internamente, el chip de una tarjeta inteligente con microprocesador se compone de:

- *CPU*: el procesador de la tarjeta; suelen ser de 8 bits aunque hay también compatibles con 16 bits, a una velocidad de reloj de 5 MHz a 66MHz y hasta 5 voltios. Pueden tener opcionalmente módulos hardware para operaciones criptográficas.
- *ROM*: memoria interna, (normalmente entre 2 y 80 KB), en la que se establece el sistema operativo de la tarjeta, las rutinas del protocolo de comunicaciones y los algoritmos de seguridad de alto nivel por software. Esta memoria, como su nombre indica, no se puede reescribir y se inicializa durante el proceso de fabricación.
- *EEPROM*: memoria de almacenamiento, (equivalente al disco duro en un ordenador personal), en el que está grabado el sistema de ficheros, los datos usados por las aplicaciones, claves de seguridad y las aplicaciones que se ejecutan en la tarjeta. El acceso a esta memoria está protegido a distintos niveles por el sistema operativo de la tarjeta.
- *RAM*: memoria volátil de trabajo del procesador y bastante limitada, su capacidad puede llegar hasta los 16 KB.

1.2. Software en tarjetas inteligentes

En la actualidad las aplicaciones que se ejecutan sobre tarjetas inteligentes son varias. Pueden ir desde aplicaciones bancarias, votos electorales, compras, identificación, seguridad social, aplicaciones telefónicas, entre otras. Sería poco conveniente que para el uso de cada uno de estos servicios el cliente tenga que poseer una tarjeta, por lo que la existencia de sistemas operativos que permitan correr múltiples aplicaciones es un paso tecnológico necesario.

Un sistema operativo de tarjeta inteligente debe encargarse de las siguientes tareas:

- Transmisión de información a través de la interfaz de comunicación serial.
- Carga, operación y administración de aplicaciones.
- Procesamiento y control de ejecución de instrucciones.
- Administración de la memoria, acceso a la información y manipulación de archivos.
- Administración y ejecución de algoritmos criptográficos.

Entre los sistemas operativos más usados en el mercado se destacan dos fundamentalmente: MultOS y Java Card.

1.2.1. MultOS

Es un sistema multiplicación para tarjetas inteligentes, forma un estándar abierto cuyo desarrollo es revisado por el MultOS Consortium. La diferencia fundamental con respecto a otros sistemas de tarjetas radica en que implementa el STEP, que es un mecanismo patentado para que la verificación de aplicaciones y la actualización en la tarjeta estén sobre el control del emisor. Es el primer sistema operativo abierto sobre tarjetas inteligentes. Posee numerosas ventajas pero tiene la limitación de ser producido por un número pequeño de compañías. Esto dificulta las necesidades de despliegue que estas plataformas llevan a cabo en la actualidad.

1.2.2. Tarjetas Java

Una tarjeta Java es una tarjeta inteligente que puede ser programada usando lenguajes de alto nivel en vez de lenguajes ensambladores. Son el último paso en las tecnologías de tarjetas inteligentes. Esto permite la realización de software mucho más fácil, además de otras ventajas como son: la portabilidad, la popularidad entre la comunidad de desarrollo y su diseño basado en applets. Los applets son pequeños trozos de código diseñados para ser montados en un cliente; esta característica las hace perfectas para la plataforma de tarjetas inteligentes.

Es una tecnología bastante madura ya que en 1997 fue presentada la primera tarjeta por varias compañías entre las que se encuentran Gemplus y Axalto [2]. La última versión de esta plataforma es la especificación 2.1.1 liberada por Sun en el año 2000.

El objetivo principal de esta tecnología es ejecutar las mismas aplicaciones en diferentes tarjetas. Para esto hace uso de una máquina virtual y unas librerías cuyas API están bien especificadas y sobre las que se ejecutan las aplicaciones. (Figura 3)

[2] Empresas líderes del Mercado en seguridad digital que se combinaron en la actual Gemalto.

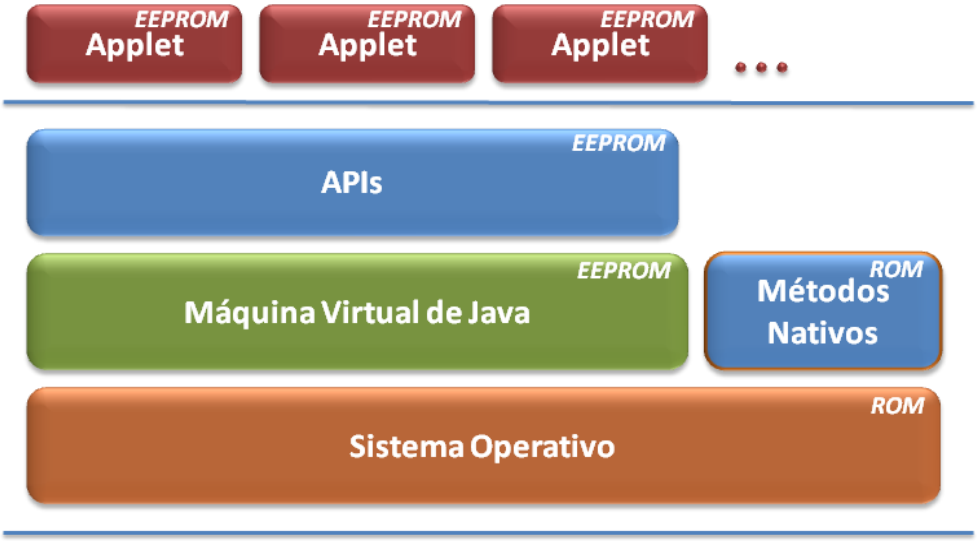

Figura 3. Estructura de una Tarjeta Java.

1.3. Componentes biométricos en tarjetas inteligentes

Las tarjetas inteligentes ofrecen una muy buena plataforma para el manejo de la información biométrica, debido a la gran seguridad de almacenamiento y procesamiento. Si una aplicación almacenara los datos biométricos en una base de datos central, la seguridad de esta comprometería la información biométrica de la población. Por otro lado si la información biométrica se almacenara en la tarjeta de cada individuo entonces ese riesgo sería mitigado. Para mayor seguridad la comparación también se realiza dentro de la tarjeta, de esta manera los datos del propietario nunca abandonarían este ambiente seguro.

La información biométrica almacenada en la tarjeta se denomina plantilla biométrica. Esta es usada en vez de la imagen biométrica que es bastante grande. La tecnología biométrica en tarjetas inteligentes usualmente extrae las características de esta imagen construyendo así una plantilla la cual es almacenada en la tarjeta, con el objetivo de disminuir el consumo de memoria. Este proceso de extracción es bastante intenso por lo que debe ser incluido en el sensor biométrico y ser manejado fuera de la tarjeta.

1.3.1. Componentes biométricos en tarjetas Java

Para la construcción de aplicaciones biométricas sobre la plataforma de tarjetas Java, existe la definición de un API que permite a las aplicaciones interactuar con los diversos componentes

de comparación biométricos existentes en el mercado. La Bio API o API biométrica para tarjetas Java fue presentada por el Java Card Forum, esta provee una interfaz uniforme de comunicación que tiene las siguientes características:

- Permite guardar de forma segura una plantilla en la tarjeta, llamada “plantilla de referencia”. Permite además verificar si una segunda plantilla o “platilla candidata” es semejante a la de referencia sin sacar los datos de la plantilla de referencia fuera de la tarjeta.
- Es simple y compacta, además de ser flexible para que permita interactuar con la variedad de algoritmos biométricos actualmente usados en la industria.
- Permite guardar múltiples plantillas biométricas en la tarjeta.
- Soporta además la funcionalidad de proteger la información biométrica y el límite de intentos fallidos de verificación.
- Reutiliza componentes de interfaces existentes como la PIN API.
- Respeta las características ya existentes para este tipo de interfaces.
- Permite el desarrollo independiente de tecnologías biométricas y clientes para esas tecnologías.

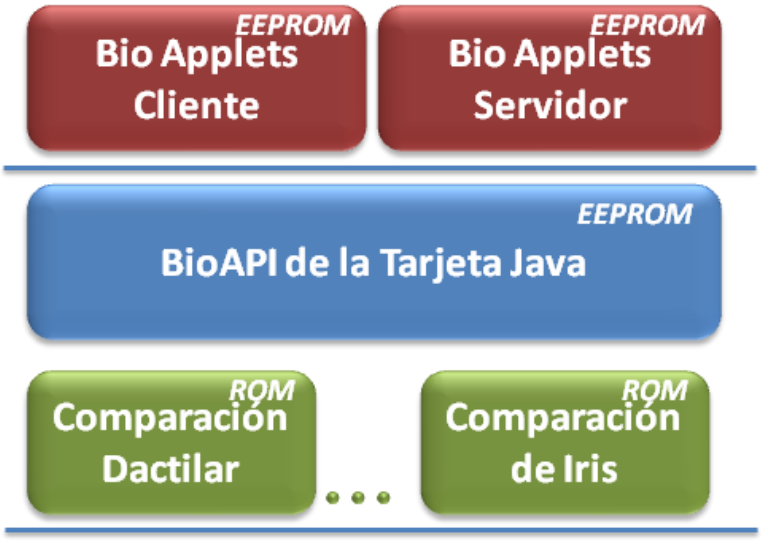

Figura 4. Arquitectura de la JC Bio API.

Esta API actúa como interfaz entre los componentes de comparación biométricos y las applets que hacen uso de estos servicios (**¡Error! No se encuentra el origen de la referencia.**). Aquí

se distinguen dos tipos: las applets servidoras, las cuales crean interfaces más personalizadas e interactúan directamente con la Bio API y las applets clientes. Estas últimas hacen uso de las servidoras para consumir este servicio biométrico.

1.4. Proceso de comparación de huellas dactilares

La comparación de huellas es una de las fases más críticas en un sistema de verificación de huellas dactilares. Comparar dos huellas puede ser un proceso muy complejo ya que en general ambas huellas habrán sufrido desplazamientos, rotaciones, transformaciones elásticas o quizás su calidad sea baja. Por lo tanto, un buen algoritmo de comparación deberá ser robusto frente a la variabilidad en las huellas a comparar.

1.4.1. Dificultades en el proceso de comparación de huellas dactilares

Las principales dificultades ante las que debe actuar un buen algoritmo de comparación son las siguientes:

- *Desplazamiento y rotación*: son el resultado de que el usuario sitúe su dedo en un lugar diferente del sensor en cada ocasión. Pueden ocasionar que una parte de la huella se encuentre fuera del área de captura, por lo que las huellas a comparar tendrán un área menor en común a la real. Este problema afecta en gran medida a los sensores con una reducida área de captura.
- *Transformación no lineal*: es la consecuencia de plasmar en una imagen de dos dimensiones una huella dactilar de 3 dimensiones, con una elasticidad que provoca deformaciones no lineales en su superficie.
- *Diferencias de presión y de las condiciones de la piel*: la presión que se ejerza contra el sensor y la humedad o sequedad de la piel, hacen que la captura sea diferente en cada situación. También afectan sustancias corporales como el sudor o la grasa.
- *Errores en la extracción de características*: los algoritmos de extracción de minucias tienden a producir minucias espurias en las huellas de baja calidad, que enmascaran a menudo las minucias reales.

1.4.2. Análisis de los algoritmos de comparación de huellas dactilares

Los algoritmos de comparación desarrollados hasta la fecha pueden clasificarse en tres grandes grupos:

- *Basados en correlación, normalmente a nivel de bloque*: las imágenes del par de huellas a comparar se superponen y se calcula la correlación entre píxeles equivalentes para diferentes alineamientos (variaciones en la posición y el ángulo).
- *Basados en minucias*: se trata de la técnica más extendida al ser la técnica en la que se sustenta la comparación manual de huellas por parte de los expertos forenses en la materia. Las minucias se extraen de ambas huellas y se almacenan en vectores como conjuntos de puntos en el plano bidimensional de la imagen. Estos algoritmos tratan de conseguir el mayor número posible de coincidencias entre pares de minucias de la huella modelo y la huella a comparar, incluso sin tener que alinear las huellas.
- *Basados en características del patrón de crestas o en texturas*: en imágenes de baja calidad la extracción de las minucias es bastante complicada y poco fiable mientras que otras características (orientación local, forma de las crestas, información de texturas), en general menos distintivas, pueden obtenerse de manera más robusta. Los algoritmos pertenecientes a esta familia comparan las huellas en términos de las características antes mencionadas extraídas del patrón de crestas.

Los métodos basados en imágenes y en textura suelen tener la dificultad de poseer plantillas de mayor tamaño. Esto representa un problema debido a la escasez de memoria que presentan las tarjetas, incluso para los grandes sistemas de identificación son un problema, ya que el almacenar millones de huellas es significativamente costoso. Otra de las características es el alineamiento, este consiste en tener ambas huellas a comparar en una misma orientación. Lograr esto puede llegar a ser un proceso bastante costoso a pesar de la existencia de diversas técnicas que hacen uso de puntos característicos como son los cores[3] y los deltas[4], pero estos tienden a ser de difícil extracción y vulnerables a los errores. Una tendencia es el uso de coordenadas relativas entre las

[3] Punto más elevado de la cresta más interna de la huella dactilar.

[4] Punto en una cresta más cercano donde dos crestas divergen.

minucias, guardándose en estructuras especializadas. Esto hace innecesario el alineamiento por lo que los algoritmos que trabajan sobre esta tendencia poseen gran ventaja.

Tabla 2 Comparación de paradigmas.

	Alineamiento	Plantilla	Rendimiento	Precisión	Sensibilidad	Adquisición
Imagen	Obligatorio	Grande	Alto	Medio	Baja	Baja
Textura	Obligatorio	Mediano	Medio	Medio	Media	Baja
Minucia	No Necesario	Muy Pequeño	Alto	Alto	Buena	Alta

1.4.3. Características particulares del proceso de comparación de huellas dactilares en tarjetas inteligentes

- *Reducida memoria de datos*: las tarjetas inteligentes son pequeños dispositivos portables, los que tienen que poseer el tamaño estándar para tarjetas, poseen muy poco espacio para agregar chips de memoria por lo que la disponibilidad de memoria dedicada para estos procesos oscila entre 2 KB y 8 KB, ya sea de RAM o EEPROM.
- *Reducida memoria de código*: estos sistemas suelen estar creados sobre APIs que son llamadas por el Applet biométrico, el cual se comunica directamente con el sistema operativo de la tarjeta. Ambos, tanto la API como el Applet comparten la memoria y en general no debe excederse de 5 KB para ambos.
- *Reducida capacidad de procesamiento*: por la miniaturización de estos chips y el reducido coste, el desempeño se ve afectado y aunque depende mucho del fabricante, estas velocidades oscilan entre 5 MHz y 100 MHz.

1.5. Estándares Existentes

El NIST contempla ampliamente los aspectos relacionados con la biometría. Para esto define estándares como parte del grupo “Elementos Biométricos para Credenciales de Identificación” (Support for Biometric Elements for Identity Credentials). En este grupo se describen los diversos estándares de la biometría entre los que se encuentra la “Biometría Dactilar” dentro de un plan que se denomina MINEX (Minutiae Exchange) que describe lo relacionado a la comparación de rasgos de huellas basada en minucias para diferentes áreas, incluida la de comparación en tarjetas inteligentes o MoC.

1.5.1. MINEX

El programa MINEX se destina a mejorar la interoperabilidad basada en plantillas biométricas. Para esto realiza un plan basado en varios ensayos, MINEX II, III y IV. Cada uno de estos integra el desarrollo, evaluación y la retroalimentación, dirigidas a las actividades de consulta entre el NIST, la industria y otras partes interesadas. Dentro del ámbito no incluye nada respecto a la gestión de la identidad basada en huellas dactilares. Los resultados están orientados a la medición de la precisión, el tiempo de procesamiento, el tamaño de plantilla y las propuestas de revisión de las normas pertinentes, además de los estudios de la utilidad de las medidas de calidad, información de calibración y de nuevas métricas.

- *MINEX I*: estas pruebas se realizaron como una primera comparación de la imagen frente a la interoperabilidad basada en minucias. Se evaluó la capacidad de algoritmos básicos para comparar las huellas dactilares de plantillas basadas en minucias, y se aprobó el formato INCITS 378 de plantillas como norma base.
- *MINEX en curso*: es un programa permanente de evaluación de interoperabilidad destinado a medir la conformidad. Utiliza extensas particiones de INCITS 378 para formular grupos interoperables de “Comparadores y Generadores de Plantillas”. Entre los clientes de estas pruebas se encuentran programas como el del Gobierno de los EE.UU. PIV el cual establece sus propios criterios sobre cómo lograr la interoperabilidad. Los resultados de estas pruebas están disponibles para cualquiera.
- *MINEX II*: está dedicado específicamente a las capacidades de los algoritmos de comparación en tarjetas. Especifica como formato de plantilla el ISO/IEC 19794-2 los que se derivan del INCITS 378:2004.
- *MINEX III*: es un programa futuro, anunciado en 2007 y aunque su alcance no está todavía bien definido se sabe que estará enfocado a la explotación de la calidad de la minucia como parte de la plantilla biométrica.

ISO/IEC 19794-2:2005 Compact Card Structure

Especifica un concepto y formatos de datos para la representación de las huellas dactilares utilizando la tendencia de minucias. Es una definición genérica, ya que puede ser utilizada en una amplia gama de áreas de aplicación cuando se trate de reconocimiento de huellas dactilares automatizado. Contiene las definiciones de los términos pertinentes, una descripción

de cómo se determinarán los puntos característicos, formatos de los datos que los contienen, tanto para uso general y para el uso en tarjetas, y la información de conformidad. Incluye tres codificaciones: Record, Normal y Compacta (**¡Error! No se encuentra el origen de la referencia.**).

Tabla 3 Formato Compacto para Tarjetas.

Descripción	Tamaño	Valor	Unidad
Coordenada X	8	[0..255]	Expresado en 0.1 mm
Coordenada Y	8	[0..255]	Expresado en 0.1 mm
Tipo de Minucia	2		
Angulo de Minucia	6	[0..63]	Granularidad de 5.625°

Define que las implementaciones de algoritmos de comparación para tarjetas inteligentes deben aceptar el formato TLV (**¡Error! No se encuentra el origen de la referencia.**).

Tabla 4 Plantilla de Minucias DO.

Tag	Longitud	Valor			
7F2E	L1	Datos Biométricos			
		Tag	**Longitud**	**Valor**	
		81	L2	Datos de las Minucias	
				Campo	Tamaño	Valor
				Coordenada X	8	[0..255]
				Coordenada Y	8	[0..255]
				Tipo de Minucia	2	
				Angulo de Minucia	6	[0..63]

Este formato también comprende otros aspectos como son la unicidad de las minucias, indicando que la tupla [X, Y, Ángulo] debe ser única, la forma de codificar las coordenadas, usando un plano X-Y semejante al que usan las computadoras y la dirección del ángulo de cada minucia que debe estar orientado en sentido contrario a las manecillas del reloj. También establece un máximo de 128 minucias dejando 384 bytes como longitud máxima de plantilla.

1.6. Sistemas existentes

1.6.1. Nivel internacional

Son pocas las empresas del mundo entero que cuentan con soluciones especializadas para la verificación dactilar en tarjetas inteligentes. El costo por incluir estos servicios en cada tarjeta

es significativo. Las necesidades crecientes para evitar el acceso de personal no autorizado, autenticar, seguros sanitarios, identificación de socios, transacciones seguras y los avances tecnológicos de los últimos 25 años hacen de una tarjeta inteligente un documento importante. Algunos sistemas biométricos son muy reconocidos y en este caso se encuentran:

SagemOrga

Algoritmos de MoC de Sagem exhibieron desde el 2004 el primer lugar en interoperabilidad y rendimiento en el MINEX I, con un muy bajo índice de error. Además de ser escalables a cualquier proveedor de tarjetas del mercado actual.

La compañía SagemOrga tiene una red de subsidiarias, oficinas de ventas y compañías en todo el mundo, siendo más significativa la producción en países como Alemania, Francia, Brasil, Rusia e India. Emplean más de 1600 personas para la especialización en tarjetas inteligentes. Además es parte del grupo de alta tecnología SAFRAN y dicho grupo genera ventas anuales de más de los 12 billones de euros y tiene 63 000 empleados en alrededor de 30 países. (6)

Oberthur Technologies / Id3 Semiconductors

Presenta el algoritmo Id3, que muestra excepcionales resultados en el rendimiento, interoperabilidad, exactitud y velocidad, mientras mantiene tasas de error por debajo de lo definido por el programa PIV del los Estados Unidos. Este algoritmo es fruto del trabajo combinado que muestran estas compañías desde 1999, cuando la primera prueba de concepto del algoritmo fue demostrada. Es importante destacar que este algoritmo muestra muy bajo consumo de memoria (menos de 1k de datos y 3k de código) lo que facilita la implementación en tarjetas. El MoC fue validado en la plataforma Java Card y ID-One de Cosmo. (7)

Oberthur Technologies muestra ventas de 882.7 millones euros en el 2008, además de ser líder mundial en el campo de las tecnologías de seguridad. (8)

Id3 Semiconductors fue fundada en 1990, es una compañía especializada en la creación y diseño de circuitos integrados, aplicaciones electrónicas y aplicaciones con énfasis en la radio frecuencia (RF), sin contacto (RFID) y despliegue de tecnologías biométricas. (9)

Precise Biometrics

Su producto principal es el MoC Precise del cual informan que es compatible con múltiples tarjetas y sistemas operativos (Java Card, MultOs). Además de brindar otros productos como son Precise BioMatch Flex Toolkit y Precise BioMatch Flex Runtime, muy vinculados a las Tarjetas Inteligentes.

Precise Biometrics es una compañía Suiza con presencia mundial, que ofrece tecnología especializada en reconocimiento de huellas dactilares y que ya ha licenciado alrededor de 80 millones de tarjetas desplegadas en 10 millones de usuarios. Desde 1999 ofrece Precise BioMatch que es su tecnología principal para leer, almacenar, y comparar huellas. Fue condecorada con el premio Frost & Sullivan del 2008. (10)

Neurotechnology

Posee un algoritmo para la comparación de huellas en la tarjeta. El MoC disponible en la versión estándar incluye software del lado de la PC. Es compatible con las especificaciones ISO/IEC 19794-2:2005. Este componente requiere una tarjeta JavaCard 2.2.1 compatible, además de 18 Kb de EEPROM libre y de 0.6 a 0.8 Kb de RAM libre. Además de estar trabajando para que este componente sea compatible en otras plataformas. La compañía asegura que obtuvo la certificación NIST MINEX y los premios Fingerprint Vendor Technology Evaluation del 2000.

Neurotechnology posee una larga lista de productos competentes que agrupa en tres grandes grupos, estos son; VeriFinger Software Development Kit (SDK), FingerCell Embedded Development Kit (EDK) y MegaMatcher Software Development Kit (SDK). Todo lo que ha hecho la empresa se basa en el agigantado paso que dio en 1998 cuando desarrolló VeriFinger, un algoritmo de identificación por huellas dactilares, diseñado para sistemas biométricos integradores. Desde entonces se han liberado 12 versiones del algoritmo, con la última de estas, VeriFinger 6.0, se presenta el algoritmo de reconocimiento por huellas dactilares más poderoso hasta la fecha. (11)

1.6.2. Nivel nacional

Solo una empresa cubana cuenta con un sistema biométrico AFIS pero ninguna tiene un componente para la comparación en tarjetas inteligentes. Aún así es importante mencionar que es la líder en Cuba en soluciones biométricas.

Datys

Datys, Tecnología y Sistemas, tiene una División destinada por completo al desarrollo de software biométrico en su software Biomesys SUITE, que desde el año 2006 ya implementa el Biomesys AFIS el cual es un sistema de reconocimiento e identificación a partir de elementos biométricos con amplia aplicación civil, permite además la realización de búsquedas rápidas de patrones en grandes bases de datos y obtuvo en la categoría de aplicaciones informáticas el "Premio de Calidad en Informática 2009", en la Feria de Informática de ese año, que se realizó en La Habana. (12)

1.6.3. Universidad de la Ciencias Informáticas

Actualmente la universidad y el Centro de Identidad no cuentan con un AFIS ni con componentes para la comparación en tarjetas, aunque en el año 2009 se presentó una tesis por parte de la facultad 7 de la universidad cuyo tema es "Algoritmo de extracción de minucias para un sistema de verificación de personas por huellas dactilares" (13) que abarcó temas relacionados como son el mejoramiento de la imagen de la huella dactilar y la extracción de las minucias. Además se encuentra en desarrollo por parte del grupo de Identidad un proyecto cuyo objetivo es la creación de un AFIS propio.

1.7. Herramientas y tecnologías empleadas

1.7.1. Visual Studio 2005

Visual Studio es un conjunto completo de herramientas de desarrollo para la generación de aplicaciones Web ASP.NET, Servicios Web XML, aplicaciones de escritorio y aplicaciones móviles. Visual Basic, Visual C++, Visual C# y Visual J# utilizan el mismo entorno de desarrollo integrado (IDE), que les permite compartir herramientas y facilita la creación de soluciones en varios lenguajes. Asimismo, dichos lenguajes aprovechan las funciones de .NET Framework,

que ofrece acceso a tecnologías, clave para simplificar el desarrollo de aplicaciones web ASP y servicios web XML. (14)

1.7.2. Microsoft Visual SourceSafe

Microsoft Visual SourceSafe es un sistema de control de versiones en el nivel de archivos, que permite a muchos tipos de organizaciones trabajar en distintas versiones de un proyecto al mismo tiempo. Esta funcionalidad es especialmente ventajosa en un entorno de desarrollo de software, donde se usa para mantener versiones de código paralelas. Sin embargo, el producto también se puede utilizar para mantener archivos en cualquier otro tipo de equipo.

Visual SourceSafe admite el desarrollo multiplataforma al permitir la edición y el uso compartido de los datos. Se ha diseñado para controlar los problemas de seguimiento y portabilidad que implica mantener una base de control de código fuente, como una base de código de software, en varios sistemas operativos. Para los desarrolladores, Visual SourceSafe aloja código reutilizable u orientado a objetos. Asimismo, facilita el seguimiento de las aplicaciones que utilizan módulos de código concretos.

1.7.3. Lenguaje C

Se trata de un lenguaje débilmente tipificado de medio nivel pero con muchas características de bajo nivel. Dispone de las estructuras típicas de los lenguajes de alto nivel pero, a su vez, dispone de construcciones del lenguaje que permiten un control a muy bajo nivel. Los compiladores suelen ofrecer extensiones al lenguaje que posibilitan mezclar código en ensamblador con código C o acceder directamente a memoria o a dispositivos periféricos. Uno de los objetivos de diseño del lenguaje C es que solo sean necesarias unas pocas instrucciones en lenguaje máquina para traducir cada elemento del lenguaje, sin que haga falta un soporte intenso en tiempo de ejecución. Es muy posible escribir C a bajo nivel de abstracción; de hecho C se usó como intermediario entre diferentes lenguajes. Es un lenguaje muy eficiente puesto que es posible utilizar sus características de bajo nivel para realizar implementaciones óptimas.

1.7.4. Lenguaje C# 2.0

Microsoft Visual C# 2005 es un lenguaje de programación diseñado para crear una amplia gama de aplicaciones que se ejecutan en .NET Framework. C# es simple, eficaz, con seguridad de tipos y orientado a objetos. Con sus diversas innovaciones, permite desarrollar aplicaciones rápidamente y mantiene la expresividad y elegancia de los lenguajes de tipo C.

La biblioteca de clases .NET Framework ofrece acceso a una amplia gama de servicios de sistema operativo y a otras clases útiles y adecuadamente diseñadas que aceleran el ciclo de desarrollo de manera significativa. (15)

1.7.5. Enterprise Architect

Enterprise Architect es una herramienta de construcción y modelado de software de alto rendimiento con una trazabilidad completa desde los requisitos iniciales hasta las decisiones de diseño de software. Provee el tipo de visualización, colaboración eficiente y robusta requerida en los entornos de desarrollo de software que son altamente demandados en la actualidad. Como una solución de modelado verdaderamente ágil, provee una sobrecarga de instalación baja, un rendimiento brillante y una interfaz intuitiva. Es una herramienta de análisis de negocio y hace uso de UML. Provee el límite competitivo para el desarrollo de software, administración de proyectos, administración de requerimientos y análisis de negocio. (16)

1.7.6. UML

Lenguaje Unificado de Modelado es el lenguaje de modelado de sistemas de software más conocido y utilizado en la actualidad. Es un lenguaje gráfico para visualizar, especificar, construir y documentar un sistema.

1.8. Metodología de desarrollo utilizada

1.8.1. Scrum y XP

Se decide optar por las metodologías ágiles Scrum y XP para el desarrollo del software debido al poco tiempo de desarrollo y el reducido grupo de trabajo. Los principales objetivos que persiguen estas metodologías son:

- Valorar al individuo y las interacciones del equipo de desarrollo sobre el proceso y las herramientas.
- Desarrollar software que funcione es más importante que conseguir una buena documentación.
- La colaboración con el cliente es más importante que la negociación de un contrato.
- Responder a los cambios es más importante que seguir estrictamente un plan.

Los principales valores que conlleva a utilizar estos métodos se expresan en el “Manifiesto Ágil”:

- La prioridad es satisfacer al cliente mediante tempranas y continuas entregas de software que le aporte un valor.
- Entregar frecuentemente software que funcione desde un par de semanas a un par de meses, con el menor intervalo de tiempo posible entre entregas.
- El software que funciona es la medida principal de progreso.
- La atención continua a la calidad técnica y al buen diseño mejora la agilidad.
- Construir el proyecto en torno a individuos motivados. Darles el entorno y el apoyo que necesitan y confiar en ellos para conseguir finalizar el trabajo.
- En intervalos regulares, el equipo reflexiona respecto a cómo llegar a ser más efectivo, y según esto ajusta su comportamiento.

La metodología Scrum:

- Define un marco para la gestión de proyectos.
- Indicada para proyectos con un rápido cambio de requisitos.
- El desarrollo de software se realiza mediante iteraciones, denominadas sprints.
- Reuniones a lo largo del proyecto.

La metodología XP:

- Centrada en potenciar las relaciones interpersonales como clave para el éxito en desarrollo de software.
- Basada en continua realimentación entre el cliente y el equipo de desarrollo.
- Simplicidad en las soluciones implementadas.

- Adecuada para proyectos con requisitos imprecisos y muy cambiantes.

Se toman elementos de Scrum y de XP y se divide en cuatro fases, que son precisamente la base de la estructura del expediente de proyecto, estas son:

- Planificación-Definición.
- Desarrollo.
- Entrega.
- Mantenimiento.

Cada una de estas fases está compuesta por una serie de actividades durante las cuales se generan los artefactos que quedan incluidos en el nuevo expediente de proyecto.

En este capítulo se mostró el análisis de todas las tecnologías involucradas para la construcción del componente así como los estándares que rigen este tipo de soluciones en la actualidad. Además de la selección de herramientas a usar dándose su descripción y la necesidad del uso de las mismas. Es importante destacar la aplicación de dos metodologías de desarrollo ágiles para lograr un desarrollo colaborativo y eficaz del componente.

CAPÍTULO 2 .CARACTERÍSTICAS DEL SISTEMA

En este capítulo se dan a conocer las principales características del sistema propuesto. Se posibilita a partir de un análisis de las singularidades abordadas, concluir cuán competente es el mismo. Además, se ofrece el modelo de dominio de la aplicación conjuntamente con la especificación de los requisitos tanto funcionales como no funcionales.

2.1. Descripción del Negocio

Dentro del campo de la biometría dactilar se identifican dos negocios fundamentales, el primero donde el proceso de comparación es realizado entre una plantilla contra muchas (1: N) que se denomina “identificación”, este está más vinculado a la criminalística y el segundo en el que la comparación ocurre solo entre dos plantillas (1: 1) y se denomina “verificación”. Este último se vincula más con el control de acceso y verificación de identidad. Precisamente es en este último se enmarca este trabajo y se identifica el siguiente flujo (Figura 5):

- El cliente introduce la tarjeta en un lector o solo la acerca en caso de sistemas sin contacto.
- Luego de establecida la conexión con la tarjeta el cliente introduce su dedo en un escáner y este extrae una imagen de su huella dactilar.
- Esta imagen obtenida es entregada al componente que se encarga de extraer las minucias y de construir la plantilla candidata. Todo este proceso es realizado fuera de la tarjeta, en la PC donde está conectado el escáner.
- Se le envía esta plantilla candidata a la tarjeta, la cual contiene en su interior la plantilla de referencia que es la que identifica al cliente y con la que se quiere establecer la similitud.
- Es realizado el proceso de comparación de las dos plantillas, la plantilla de referencia que se encuentra todo el tiempo en la tarjeta y la plantilla candidata que es la que se envía y con la que se intenta verificar. Este proceso se realiza dentro de la tarjeta y arroja un valor de similitud con el que queda asegurada la autenticación.

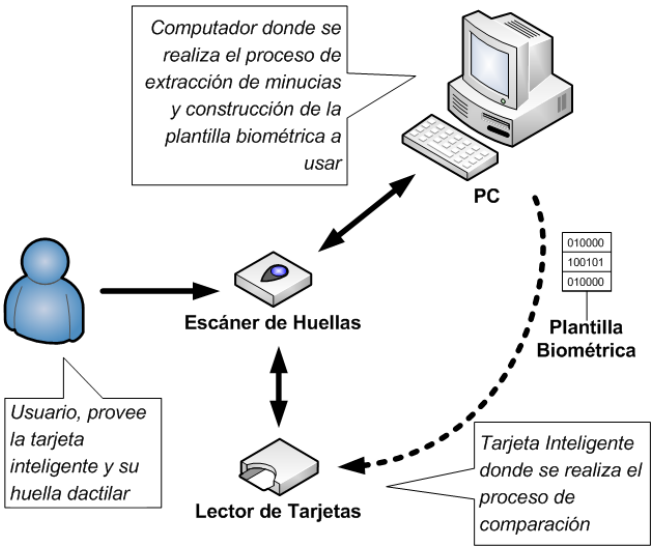

Figura 5. Flujo de Trabajo.

Esta modalidad de verificación se denomina por sus siglas MoC o Comparación en Tarjeta, que brinda las siguientes ventajas:

- Las tarjetas son de presencia obligatoria, pues para establecer la identidad de un cliente, tanto él como la tarjeta tienen que estar en el mismo lugar en un mismo momento, lo que permite asegurar también la presencia física del cliente.
- Esta tecnología está aprobada por el certificado 140-2.
- No necesita de una base de datos centralizada.
- La referencia biométrica nunca abandona la tarjeta por lo que mantiene la confidencialidad de esta información.

2.2. Descripción del Problema

El Centro de Identificación y Seguridad Digital de la Universidad de las Ciencias Informáticas, está involucrado en el despliegue de cédulas de identificación electrónicas para la hermana República Bolivariana de Venezuela. Esto ha sido parte del Proyecto de Modernización del Sistema de Identificación, Migración y Extranjería, en el cual las autoridades venezolanas acuerdan la utilización de un documento de identificación soportado sobre tarjetas inteligentes para fortalecer dicho sistema. Estas cédulas electrónicas son tarjetas inteligentes las cuales deben realizar la identificación biométrica con un componente de comparación. Este componente es comprado para cada tarjeta por lo que representa un gran valor al mencionar

que el despliegue está por la cifra de millones de cédulas. De realizarse este componente en la UCI abarataría considerablemente los costos siendo esto un ahorro considerable para el país.

2.3. Análisis de tendencias existentes

Dado que el consumo de memoria en las tarjetas inteligentes es un punto fundamental, arroja como paradigma ideal el basado en minucias, precisamente porque implica un tamaño mínimo de plantilla biométrica. El uso de plantillas biométricas está especificado por el MINEX II el cual recomienda el uso del estándar: ISO/IEC 19794-2:2005 Compact Card Structure, que es un formato que guarda de la forma más compacta posible lo relativo a las minucias de la huella. El formato de plantillas biométricas a usar es un punto clave en el desarrollo del algoritmo de comparación. De ahí se enmarcan dos tendencias:

- *Formato ISO*: usa el formato estándar propuesto por el MINEX II. Su principal ventaja es que no está atado al componente de extracción ya que dichos componentes están obligados a implementar este como mínimo. Esta característica les permite una mayor penetración en el mercado debido a su gran compatibilidad. Como principal dificultad pueden encontrarse problemas de rendimiento, ya que desarrollar un algoritmo con estas plantillas conlleva a un gran trabajo de optimizaciones, esto hace el comienzo mucho más difícil.
- *Formato Privado*: aquí el creador del componente decide cual va a ser el formato que tendrá su plantilla, para así aprovecharlo al máximo explorando nuevas posibilidades, ya que este proceso es realizado en una PC convencional y no posee las limitaciones que implica una tarjeta inteligente, pudiendo desarrollar para esta labor procesos de mucha mayor complejidad y liberar así a la tarjeta de estos trabajos. La principal dificultad consiste en la estrecha vinculación que esto impone con el componente de extracción de rasgos o características, ya que también se deberá proveer uno que genere estas plantillas, limitando así la compatibilidad.

2.4. Propuesta del sistema

El sistema propuesto consta de un componente en el cual se realiza la comparación de huellas dactilares en la plataforma de tarjetas inteligentes. Este proceso recibe como entrada dos plantillas para las cuales se debe definir un formato a usar, ya sea estándar o propio. Como

resultado debe arrojar una puntuación que indica la medida de semejanza entre estas dos plantillas. Además deben especificarse los umbrales para los cuales se obtiene la mejor precisión.

2.5. Objeto de automatización

El componente permite la comparación automática de los rasgos de las huellas dactilares. Si este componente no existiera dicha comparación se realizaría de la forma tradicional, donde un perito examina exhaustivamente la imagen de la huella buscando semejanzas entre las minucias. Se menciona que según datos experimentales dichos peritos solo tienen que identificar la relación entre 12 minucias para confirmar que un par de huellas son iguales. Esto puede tomar demasiado tiempo, además de no poderse contar con un experto en cada local que se requiera un acceso controlado. De ahí surge la necesidad de automatización, siendo esto de vital importancia para el desarrollo y la aplicación grandes sistemas de seguridad.

2.6. Modelo de dominio

En el modelo de dominio (Figura 6) se muestra la relación existente entre los conceptos fundamentales de este tipo de sistemas. Aquí se observa como el componente de comparación está en cada tarjeta y como la tarjeta cuenta con una plantilla de referencia la cual se compara con otra candidata. En la práctica, una tarjeta puede tener una plantilla de referencia para cada dedo y se verifican varios de ellos en dependencia del nivel de seguridad que se quiera lograr. Esta autentificación puede estar incluso combinada con un PIN o con otro sistema biométrico. Las plantillas contienen el contenido de las minucias de la huella dactilar y pueden tener además otra información en caso de las plantillas privadas.

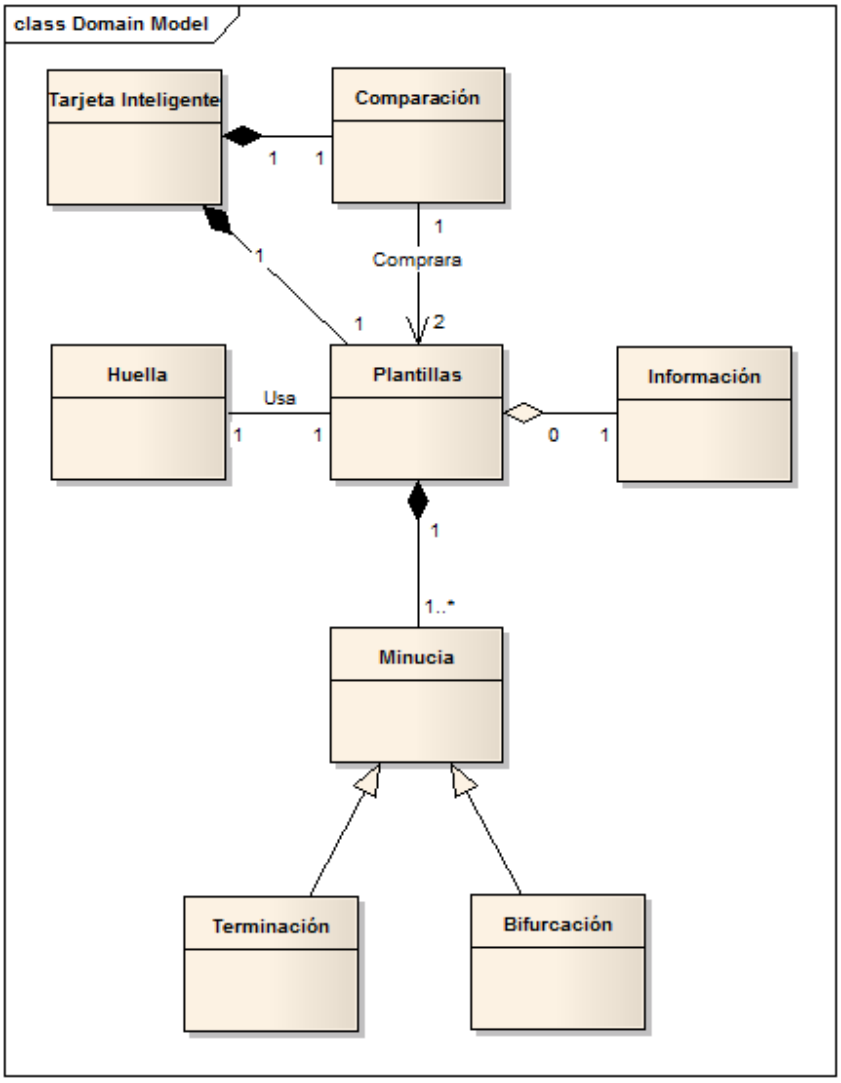

Figura 6. Modelo de Dominio.

2.7. Lista de reserva del producto

Es una lista priorizada que define el trabajo que se va a realizar en el proyecto. Cuando un proyecto comienza es muy difícil tener claro todos los requisitos sobre el producto. Sin embargo, suelen surgir los más importantes que casi siempre son más que suficientes para un Sprint (Iteración). Esta lista puede crecer y modificarse a medida que se obtiene más conocimiento acerca del producto y del cliente. Con la restricción de que solo puede cambiarse entre Sprint. El objetivo es asegurar que el producto definido al terminar la lista es el más

correcto, útil y competitivo posible y para esto la lista debe acompañar los cambios en el entorno y el producto.

2.7.1. Funcionalidades del sistema

Tabla 5 Funcionalidades del Sistema.

No.	Funcionalidad	Prioridad
1	Definir la plantilla a usar	Alta
2	Comparar las plantillas	Alta
3	Validación de las plantillas de entrada	Media
4	Permitir la interrupción de la comparación	Media

2.7.2. Requisitos no funcionales del sistema

Requisitos de Rendimiento:

- La longitud del código no debe exceder los 5 KB de EEPROM.
- La longitud de los datos en EEPROM no debe exceder los 5 KB compartidos con el código.
- Los datos almacenados en RAM por el algoritmo no deben exceder los 2KB.
- El tiempo de ejecución debe ser negociado con el cliente, pero nunca mayor de los 10 segundos.

Requisitos de Software:

- El componente debe ser compatible con la plataforma JC 2.2.1 smartcard OS.

Requisitos de Hardware:

- El componente debe ser compatible con el chip IFX SLE66CLX800 PE, usado en las cédulas electrónicas.

Restricciones en el Diseño y en la Implementación:

- La implementación del componente debe ser desarrollada en el lenguaje C.

- El diseño del sistema debe ser compatible con las especificaciones entregadas por los clientes las cuales imponen una interfaz a ser usada para la correcta de comunicación con la BIO API.

2.8. Historias de usuarios

Las historias de usuarios son la técnica utilizada para especificar los requisitos del software, lo que equivale a los casos de uso en el Proceso Unificado. Las mismas son escritas por los clientes como las tareas que el sistema debe hacer.

Tabla 6 Historia de Usuario 1

Historia de Usuario	
Numero: 1	**Nombre de Historia de Usuario:** Definir la plantilla a usar.
Modificación de Historia de Usuario Número: ninguna	
Usuario: BIO API	**Iteración Asignada:** 1
Prioridad en Negocio: Alta	**Puntos Estimados:** 2 semanas
Riesgo en Desarrollo: Alto	**Puntos Reales:** 2 semanas
Descripción: A partir de una imagen de un escáner se define una plantilla, se construye la información que el componente de comparación necesita para realizar su proceso dentro de la tarjeta, lo cual está estrechamente vinculado al algoritmo diseñado.	
Programador Responsable: Raúl Ballester	

Tabla 7 Historia de Usuario 2

Historia de Usuario	
Numero: 2	**Nombre de Historia de Usuario:** Comparar las plantillas.
Modificación de Historia de Usuario Número: ninguna	
Usuario: BIO API	**Iteración Asignada:** 2
Prioridad en Negocio: Alta	**Puntos Estimados:** 2 semanas
Riesgo en Desarrollo: Alto	**Puntos Reales:** 2 semanas
Descripción: Se comparan las huellas con el algoritmo diseñado, usando la información de las platillas previamente definidas.	
Programador Responsable: Abel Sánchez	

Tabla 8 Historia de Usuario 3

Historia de Usuario	
Numero: 3	**Nombre de Historia de Usuario:** Validación de las plantillas de entrada.
Modificación de Historia de Usuario Número: ninguna	

Usuario: BIO API	**Iteración Asignada:** 3
Prioridad en Negocio: Media	**Puntos Estimados:** 1 semana
Riesgo en Desarrollo: Bajo	**Puntos Reales:** 1 semanas
Descripción: Se valida que el componente se comporte correctamente ante plantillas con errores.	
Programador Responsable: Raúl Ballester	

Tabla 9 Historia de Usuario 4

Historia de Usuario	
Numero: 4	**Nombre de Historia de Usuario:** Permitir la interrupción de la comparación.
Modificación de Historia de Usuario Número: ninguna	
Usuario: BIO API	**Iteración Asignada:** 3
Prioridad en Negocio: Media	**Puntos Estimados:** 1 semanas
Riesgo en Desarrollo: Medio	**Puntos Reales:** 1 semanas
Descripción: Ajustar el algoritmo para que sea interrumpible.	
Programador Responsable: Abel Sánchez	

2.9. Plan de entregas

Una vez obtenida la concepción del sistema, definidas dichas funcionalidades y agrupadas por historias de usuarios se define el plan de entregas donde se muestran las iteraciones para realizar las entregas intermedias y final de cada funcionalidad del sistema y su duración en semanas. De acuerdo a la prioridad definida por funcionalidades e interés del cliente se realizó la siguiente planificación:

Tabla 10 Plan de Entregas

Entrega	Descripción de la Iteración	Orden de Historia de Usuario	Duración
1	Definir plantillas de comparación	1	2
2	Comparar plantillas	2	2
3	Validar y Refinar la comparación	3, 4	2

2.10. Descripción de la arquitectura

La arquitectura a usar está limitada por los clientes, expuestas en el documento de especificaciones entregadas al proyecto. Consta de la implementación en C de los siguientes métodos para formar parte de la API nativa de la tarjeta inteligente:

Tabla 11 Prototipo de MoC_SetWorkingBuffer

Prototipo	
void MoC_SetWorkingBuffer(uint8 __ram__ * p_Buffer)	
Propósito	
Este método se invoca antes de cualquier llamada con el objetivo de inicializar el buffer para obtener la respuesta.	
Parámetros	**Descripción**
p_Buffer	Un puntero a la memoria que será usada como buffer para realizar el enrolamiento, verificación u otra operación.

Tabla 12 Prototipo de MoC_Transform

Prototipo	
uint16 MoC_Transform(uint8 * p_Minutiae_Template_DO, uint16 u16_TemplateSize, uint16 * p_Size_Internal_Format)	
Propósito	
Este método es invocado para enrolar una plantilla de referencia. Algunos pre-cálculos pueden ser hechos con el objetivo de acelerar la comparación. La plantilla transformada debe ser copiada en el offset 0 del buffer previamente definido por el método *MoC_SetWorkingBuffer.*	
Parámetros	**Descripción**
p_Minutiae_Template_DO	Puntero a la plantilla biométrica ISO.
u16_TemplateSize	Representa la longitud en bytes de la lista de minucias pasada, y como cada minucia lleva 3 bytes, la cantidad de minucias está dada por la división de este valor entre 3.
p_Size_Internal_Format	Puntero a un uint16 que debe contener la longitud en bytes de la plantilla en el formato interno.
Devuelve un valor con el estado de la ejecución de este método.	

Tabla 13 Prototipo de MoC_Verify

Prototipo	
uint16 MoC_Verify(uint8 * p_Reference, uint8 * p_Candidate, uint16 u16_CandidateTemplateSize, uint16 * p_Matching_Score)	
Propósito	
Este método es invocado para realizar la comparación de la plantilla candidata con la plantilla previamente enrolada. La RAM puede ser previamente inicializada con el método *MoC_SetWorkingBuffer.*	
Parámetros	**Descripción**
p_Reference	Puntero a la plantilla previamente enrolada, el formato de esta plantilla ya estará codificado con el formato interno.
p_Candidate	Puntero a la plantilla candidata que estará codificada usando

	el formato ISO.
u16_CandidateTemplateSize	Longitud en bytes de la plantilla candidata.
p_Matching_Score	Puntero a un uint16 que debe contener la puntuación de la comparación con el orden de establecer la semejanza entre las plantillas comparadas.
Devuelve un valor con el estado de la ejecución de este método.	

Tabla 14 Prototipo de MoC_GetAlgoVersion

Prototipo
uint16 MoC_GetAlgoVersion(void)
Propósito
Este método es usado con objetivos de rastreo, con la razón de distinguir la versión del algoritmo usado.
Devuelve un valor que representa la versión del algoritmo.

Tabla 15 Códigos de Retorno

Error	**Descripción**
C5C5h	Sin error.

En este capítulo se exponen las tendencias a MoC a usar y se concluye que para la construcción de este componente se hará uso de una plantilla propietaria. Se muestran todos los requisitos funcionales y no funcionales además de las condiciones de diseño impuesta por los fabricantes de las tarjetas. Lo que evidencia la rigurosidad con que se desarrollan estos componentes, dada las condiciones de alta competitividad que ha alcanzado la biometría dactilar en la actualidad.

CAPÍTULO 3. DESARROLLO DEL SISTEMA

En este capítulo se aborda el diseño de la plantilla biométrica propuesta para el algoritmo, se describe brevemente el mismo y se define el estilo de codificación a usar. Además se realiza el diseño de pruebas y se dan a conocer los resultados obtenidos de las mismas.

3.1. Diseño algorítmico

3.1.1. Diseño de la plantilla a usar

La plantilla a usar es basada en una estructura diseñada para ser invariante a traslación y rotación. Para cada minucia se guarda la información relativa a *k* minucias cercanas con el orden de tener información de su vecindad. Estas estructuras en forma de estrella se les llaman Kplet (Figura 7) y son calculadas para cada minucia de la huella.

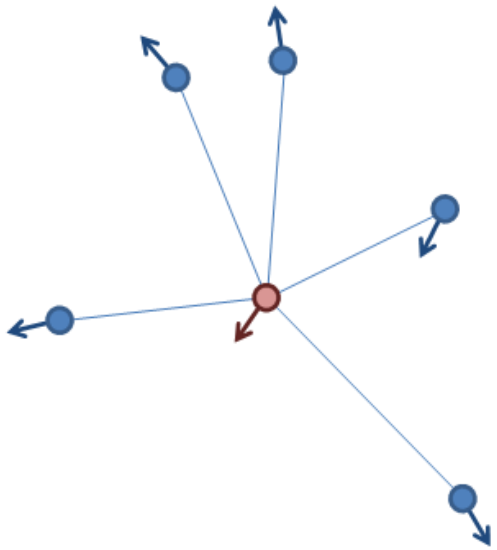

Figura 7. Estructura del Kplet.

Para cada minucia de la vecindad se guardan los siguientes valores con el objetivo de garantizar que esta estructura se invariante a la rotación y a la traslación:

- Ángulo1: ángulo formado por la orientación de la minucia central y el segmento que la une con la minucia vecina actual.
- Ángulo2: ángulo formado por la orientación de la minucia vecina y el segmento que la une con la minucia central.
- Distancia: distancia euclidiana entre la minucia central y la vecina actual.
- Surcos*:* Cantidad de surcos que se encuentran en la huella entre las minucia central y la vecina actual.

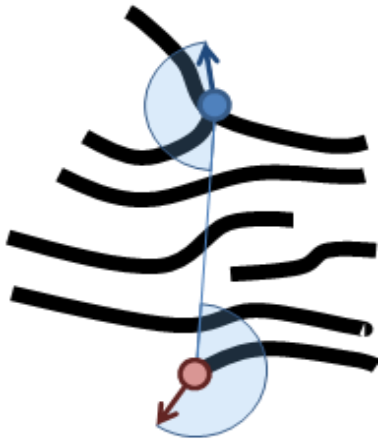

Figura 8. Datos de Vecindad.

3.1.2. Descripción del algoritmo

El algoritmo a usar realiza la comparación entre las informaciones de vecindad presentes en cada huella. La similitud obtenida es representada por un valor entre 0 y 1 que es llamado puntuación para la cual se debe determinar el umbral óptimo a usar.

3.2. Estilo de codificación

Para conseguir que el código pueda ser entendido y modificado fácilmente por cada miembro del equipo es imprescindible el uso de un estilo de codificación. Una codificación bien definida logra que todo el equipo se sienta cómodo con el código escrito por cualquier otro miembro del equipo. El estilo definido en este trabajo es el siguiente:

Se contemplaron tres estilos de capitalización distintos, que se utilizan en determinados casos:

- Capitalización Pascal: en este estilo se capitaliza la primera letra de cada palabra (*OnCard*), usada en la declaración de métodos.
- Capitalización Camel: en este otro estilo se capitaliza la primera letra de cada palabra excepto la primera (*onCard*), usada en la declaración de variables.
- Capitalización Versa: es aquella en la que todo se escribe en mayúsculas (*ONCARD*), usada en la declaración de constantes.

Sentencias simples:

- Cada línea contendrá no más de una sentencia, aunque una sentencia sí puede estar en más de una línea.

Los comentarios:

- Deben ser suficientes para mejorar el entendimiento del código (no demasiados).
- Se utilizará solamente el formato //, nunca se utilizará el /*...*/. Cuando haya que comentar un bloque de líneas, se utilizarán tantos // al principio de línea como convenga.

Otros:

- Evitar expresiones innecesariamente complejas.
- Tabulación de cuatro espacios.
- No abusar de los operadores lógicos de negación.
- Evitar anidamientos profundos.
- Usar los paréntesis para una mejor comprensión de las expresiones.
- Codificar de forma legible para los demás miembros del equipo.

3.2.1. Ejemplo de código

```
const uint8 MAX = 63; //máximo número de minucias

//método invocado para enrolar una plantilla de referencia
//la plantilla transformada debe ser copiada en el offset 0 del buffer
//previamente definido por el método MoCSetWorkingBuffer
uint16 MoCTransform(uint8 * pMinutiaeTemplateDO, uint16 u16TemplateSize,
uint16 * pSizeInternalFormat)
{
```

```
    uint16 returnState = 0xC5C5;
    ....
    return returnState;

}
```

3.3. Diseño de pruebas

Un aspecto importante de rendimiento en los sistemas biométricos es la precisión en el proceso de identificación. En la literatura se consideran tres parámetros que ayudan a determinar dicha precisión de una manera cuantitativa (17):

- Tasa de falso rechazo (FRR): es el porcentaje de usuarios autorizados que tratan de acceder al sistema y este los declara como no autorizados.
- Tasa de falsa aceptación (FAR): es el porcentaje de intentos de accesos de usuarios no autorizados los cuáles el sistema acepta como autorizados.
- Tasa de igualdad de error (ERR): es el punto en el cuál FRR y FAR son el mismo valor.

Estos valores estadísticos son calculados a partir de una muestra de imágenes de huellas dactilares. Se seleccionó de una base de datos de ciudadanos, una cantidad de 2000 huellas cada una con 2 tomas, para un total de 4000 huellas.

Se desarrolló una aplicación auxiliar para la automatización del proceso de cómputo de estos indicadores. Dicha aplicación separa las 4000 huellas en 2 grupos, el primer grupo con las tomas originales y el segundo con las segundas tomas. Cada huella del primer grupo se comparara con cada una del segundo, realizándose así 2000^2 comparaciones.

Para cada comparación el algoritmo devuelve un valor real entre 0 y 1. Este valor es denominado puntuación o score de la similitud entre las huellas comparadas. Para establecer la aceptación este valor es comparado con un umbral determinado. Si se encuentra por encima entonces se consideran semejantes de lo contrario son rechazadas.

$$puntuación = Comparar(huellaA, huellaB) \begin{cases} puntuación \geq umbral & : \ Aceptada \\ puntuación < umbral & : \ Rechazada \end{cases}$$

$$puntuacion \in R, \qquad 0 \leq valor \leq 1$$

Para cada comparación realizada se analiza como umbral valores en el intervalo unario y para cada umbral se calculan los indicadores FAR y FRR. Debido a que las huellas contienen identificadores, a la aplicación le es posible determinar cuándo es correcto un rechazo o una aceptación. Se obtienen inicialmente dos gráficas, FAR y FRR, en función de un umbral. Finalmente estas funciones son interceptadas y el punto donde se interceptan representa el umbral óptimo a usar y el valor de ese punto es el ERR. Esto es visualizado en una tercera grafica cruzada.

3.4. Resultados obtenidos

Los resultados obtenidos mediante las pruebas realizadas arrojan un ERR de 9.67% para un umbral de 0.75 donde el funcionamiento del componente se considera óptimo. (Figura 9)

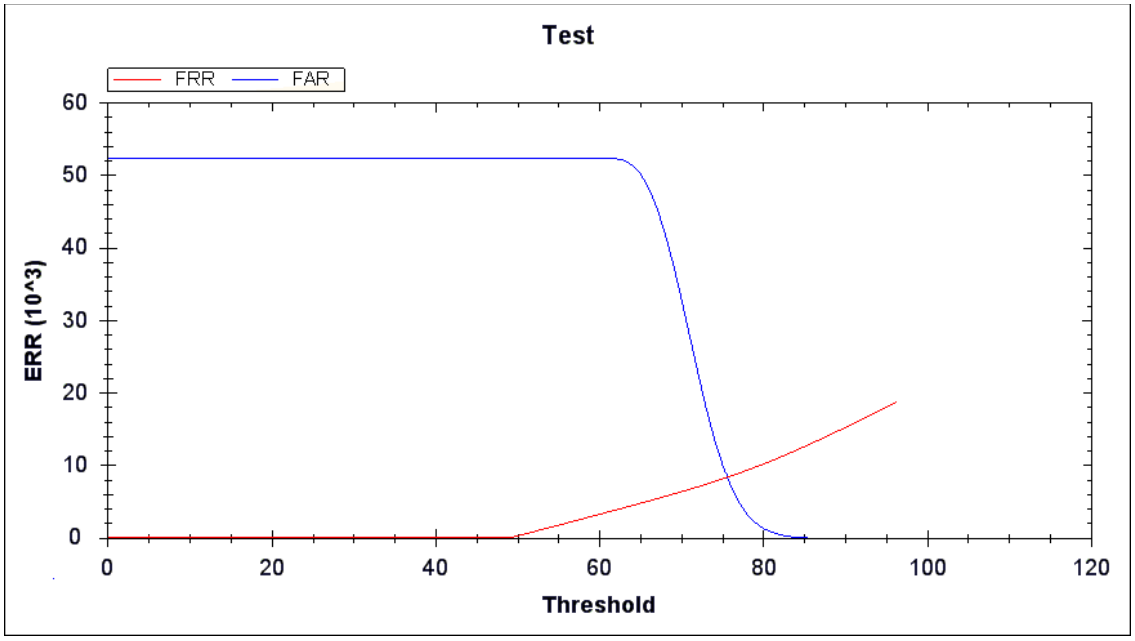

Figura 9. Curvas FAR y FRR obtenidas.

Se comparan los resultados con los datos de las pruebas experimentales realizadas a un sistema basado en tarjeta inteligente (cuyo algoritmo de comparación es desconocido) y estas arrojaron un ERR de 9.78%. Lo anterior demuestra un comportamiento similar al funcionamiento del componente desarrollado.

En este capítulo se mostró la descripción más especifica posible del las características del algoritmo de comparación a usar en el componente y además el diseño de la plantilla con que este trabaja. Es importante mencionar que el contenido de involucra la descripción del algoritmo no puede ser mostrado, por la política del Centro de Identidad y Seguridad Digital del cual este algoritmo es propiedad intelectual.

CONCLUSIONES

En este trabajo se concluye que:

- Se dotó al Centro de Identificación y Seguridad Digital de la Universidad de las Ciencias Informáticas de un componente de comparación de huellas dactilares en tarjetas inteligentes, una de las tecnologías más novedosas en los campos de la biometría.
- El componente desarrollado cumple con los estándares internacionales, es altamente competitivo y por sus funcionalidades sienta las bases para la elaboración de un AFIS. Será posteriormente implantado en las cédulas de identificación electrónicas en la hermana República Bolivariana de Venezuela, lo que representa un ahorro de divisa significativo para Cuba por concepto de importación de software.

RECOMENDACIONES

Los autores recomiendan:

- Realizar pruebas de rendimiento al componente con el objetivo de mejorar el tiempo de ejecución del mismo.
- Realizar pruebas de eficiencia al componente en un entorno real para tarjetas inteligentes, ya sea en un emulador o dentro de la tarjeta.
- Realizar un componente para la comparación de huellas dactilares en tarjetas inteligentes que utilice como entrada la plantilla ISO.

GLOSARIO DE TÉRMINOS

Algoritmo	Conjunto ordenado y finito de operaciones que permite hallar la solución de un problema. Un conjunto prescrito de instrucciones o reglas bien definidas, ordenadas y finitas que permite realizar una actividad mediante pasos sucesivos que no generen dudas a quien lo ejecute.
Enrolar	Inscribir a un individuo en una lista o rol de tripulantes de un barco mercante. Refiere a la inscripción de la plantilla biométrica del individuo en la tarjeta. Este proceso es realizado una sola vez en el momento de fabricación.
Euclidiana	Refiriéndose a Geometría Euclidiana. Es aquella que estudia las propiedades del plano y el espacio tridimensional.
Umbral	El umbral es la cantidad mínima de señal que ha de estar presente para ser registrada por un sistema.

REFERENCIA

1. **Arenas Paz, Natalia del Rosario.** Monografias. [Online] http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas.shtml.

2. **Peredo, Alvaro.** Aprende Gratis. [Online] http://www.aprendergratis.com/dactiloscopia-identificacion-de-sospechosos-y-el-futuro.html.

3. **2, Ibidem.**

4. *Diseño e Implementación de un prototipo para un sistema de control de venta de gas licuado de petróleo utilizando tarjetas inteligentes y terminales de aplicaciones bancarias.* **Renato Escobar, Pablo.** Quito : Escuela Politécnica Nacional, Marzo 2009.

5. **4, Ibidem.**

6. **Sagen Orga Web Site.** Sagen Orga Web Site. *Sagen Orga Web Site.* [Online] Sagen Orga. www.sagem-orga.com.

7. **All Pay News.** All Pay News Web Site. [Online] http://www.allpaynews.com/content/oberthurid3-fingerprint-on-card-comparison-biometrics-meets-nist-criteria.

8. **Oberthur Web Site.** Oberthur Web Site. *Oberthur Web Site.* [Online] http://www.oberthur.com.

9. **Id3.** Id3 Web Site. [Online] http://www.id3.eu.

10. **Precise Biometrics Web Site.** Precise Biometrics Web Site. *Precise Biometrics Web Site.* [Online] http://www.precisebiometrics.com.

11. **Neurotechnology Web Site.** Neurotechnology Web Site. *Neurotechnology Web Site.* [Online] http://www.neurotechnology.com/.

12. **Datys.** Biomesys AFIS: Premio de Calidad en Informática 2009. [Online] http://www.datys.cu/wpinfnoticias.aspx?94%27.

13. **Arias González, Yerandy and Leyva Morales, Alexander.** Algoritmo de extracción de minucias para un sistema de verificación de personas por huellas dactilares. Ciudad de La Habana : Universidad de las Ciencias Informáticas, 2009.

14. **Microsoft.** MSDN Web Site. *MSDN Web Site.* [Online] http://msdn.microsoft.com/.

15. **12, Ibidem.**

16. **Sparx Systems.** Sparx Systems Web Site. *Sparx Systems Web Site.* [Online] http://www.sparxsystems.com.ar/new/products/index.php.

17. *Vulnerabilidades en Sistemas de Reconocimientos Basados en Huellas Dactilares, Ataques Hill-Climbing.* **Martínez Días, Marcos.** Madrid : Universidad Autonoma de Madrid, 2007.

BIBLIOGRAFÍA

1. **Arenas Paz, Natalia del Rosario.** Monografias. [Online] http://www.monografias.com/trabajos57/huellas-lofoscopicas/huellas-lofoscopicas.shtml.

2. **Arias González, Yerandy and Leyva Morales, Alexander.** Algoritmo de extracción de minucias para un sistema de verificación de personas por huellas dactilares. Ciudad de La Habana : Universidad de las Ciencias Informáticas, 2009.

3. *A Hybrid Fingerprint Matcher.* **Arun Ross, Anil Jain, James Reisman.** Quebec City : Michigan State University, Siemens Corporate Research, Inc., 2002.

4. *A Correlation-Based Fingerprint Verification System.* **Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez,Leo P.J. Veelenturf and Berend Jan van der Zwaag.** Veldhoven, Holanda : University of Twente, Department of Electrical Engineering, Laboratory of Signals and Systems, 2000.

5. *Minutiae-based Methods.* **D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar.** New York : Springer Verlag, 2003.

6. *Fingerprint Matching Using an Orientation-Based Minutia.* **Marius Tico, Pauli Kuosmanen.** 8, s.l. : IEEE transactions on pattern analysis ane machine intelligence, 2003, Vol. 25.

7. *Vulnerabilidades en Sistemas de Reconocimientos Basados en Huellas Dactilares, Ataques Hill-Climbing.* **Martínez Días, Marcos.** Madrid : Universidad Autonoma de Madrid, 2007.

8. **Morales L., Domingo and Ruiz del Solar, Javier.** Pontificia Universidad Católica de Chile. [Online] http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm.

9. *Fingerprint Matching using Gabor Filters.* **Muhammad Umer Munir, Muhammad Younas Javed.** Rawalpindi, Pakistan : College of Electrical and Mechanical Engineering, National University of Sciences and Technology, 2004.

10. **Peredo, Alvaro.** Aprende Gratis. [Online] http://www.aprendergratis.com/dactiloscopia-identificacion-de-sospechosos-y-el-futuro.html.

11. **Pérez Costa, Michel Rafael and Fernández Leyva, Luis.** Sistema de Administración de Tarjetas Inteligentes y Aplicaciones para la Cédula de Identidad Electrónica de la República Bolivariana de Venezuela. Habana : Universidad de las Ciencias Informáticas, 2008.

12. *Diseño e Implementación de un prototipo para un sistema de control de venta de gas licuado de petróleo utilizando tarjetas inteligentes y terminales de aplicaciones bancarias.* **Renato Escobar, Pablo.** Quito : Escuela Politécnica Nacional, Marzo 2009.

13. *Mecanismos de Autenticación Biométrica Mediante Tarjeta Inteligente.* **Sánchez Reillo, Raúl.** Tesis Doctoral, Madrid : Escuela Técnica Superior de Ingenieros de Telecomunicación, 2000.

14. **Vázquez Aragón, Elvis and Fuentes Lora, Yuri G.** Prototipo de aplicación para la gestión de información. s.l. : Universidad de las Ciencias Informáticas, 2007.

15. **All Pay News.** All Pay News Web Site. [Online] http://www.allpaynews.com/content/oberthurid3-fingerprint-on-card-comparison-biometrics-meets-nist-criteria.

16. **Datys.** Biomesys AFIS: Premio de Calidad en Informática 2009. [Online] http://www.datys.cu/wpinfnoticias.aspx?94%27.

17. **Id3.** Id3 Web Site. [Online] http://www.id3.eu.

18. **Biometric Consortium.** *Java Card Biometric API White Paper.* s.l. : NIST/Biometric Consortium, 2002. 02-0016.

19. **Microsoft.** MSDN Web Site. *MSDN Web Site.* [Online] http://msdn.microsoft.com/.

20. **Neurotechnology Web Site.** Neurotechnology Web Site. *Neurotechnology Web Site.* [Online] http://www.neurotechnology.com/.

21. **Oberthur Web Site.** Oberthur Web Site. *Oberthur Web Site.* [Online] http://www.oberthur.com.

22. **Precise Biometrics Web Site.** Precise Biometrics Web Site. *Precise Biometrics Web Site.* [Online] http://www.precisebiometrics.com.

23. **Sagen Orga Web Site.** Sagen Orga Web Site. *Sagen Orga Web Site.* [Online] Sagen Orga. www.sagem-orga.com.

24. **Sparx Systems.** Sparx Systems Web Site. *Sparx Systems Web Site.* [Online] http://www.sparxsystems.com.ar/new/products/index.php.