Universidad de las Ciencias Informáticas
Facultad #4

Título: Integración biométrica para la Identificación en el proyecto SIGEP

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

Autor:

Nolber Martínez Zamora

Tutor:

Lic. Wilbert Peña Vega

Ciudad de la Habana

Julio, 2007

DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo al Sistema de Gestión Penitenciaria de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmamos la presente a los ____ días del mes de _____ del año _____.

_____

Autor: Nolber Martínez Zamora

_____

Tutor: Lic. Wilbert Peña Vega

Por motivos de conformidad con el proveedor; no se puede divulgar la información relacionada con los dispositivos y medios usados en el desarrollo. Por lo queda la divulgación prohibida; significa que la persona que reciba este documento no está autorizado para transmitir ninguna de la información contenida en él, cualquiera que sea la forma: oralmente, por red de computador, teléfono, diapositivas, fotografías, cintas de video, etcétera. La divulgación está limitada a las personas relacionadas con este documento para el uso declarado en el contrato existente entre Sagem Défense Sécurité y el receptor externo.

A mi madre por su apoyo incondicional.

A mis compañeros en especial a Yanay, Michel, Yanetsi, Yunior, René, Leuris, Rafael, Yosbel, Yoenia que me bridaron su apoyo y amistad.

A todos, gracias

A Nena, Edael, Tamara, Raúl y Nurvis

Por ayudarme durante estos largos años de universidad.

A mi hijo Pablo Maidier

Con todo el corazón.

El uso de la identificación basada en métodos biométricos es uno de los campos de más auge en la industria informática de la actualidad. La necesidad de mantener identificadas a las personas en cualquier ámbito de la vida es uno de los retos que se trazan los gobiernos e instituciones; y es precisamente uno de los principales problemas que se presentan al desarrollar un producto para la gestión de personas.

Esta tesis aborda las tecnologías actuales de identificación por medios biométricos, enmarcándose en el uso de ella para la identificación de los individuos privados de libertad en las prisiones de la República Bolivariana de Venezuela. Tiene como objetivo integrar un módulo de identificación biométrica dentro del Subsistema de Datos Personales del SIGEP. Para esto se incluye el uso del paquete XLS2 del proveedor SAGEM.

Palabras claves

Biometría, PK, AFIS, SAGEM, XLS2, MSO, Booking, SGM

TABLA DE CONTENIDOS

Introducción 1

Capítulo 1: Fundamentación Teórica 4

1.1 Identificación y reconocimiento de personas 4

1.2 Características biométricas de los individuos que facilitan su identificación 5

1.2.1 Concepto de biometría 6

1.2.2 Rasgos característicos e indicadores biométricos 7

1.3 Tecnologías 11

1.3.1 Reconocimiento por Huellas Digitales 12

1.3.2 Reconocimiento facial 17

1.3.3 Sistemas de verificación de voz 20

1.3.4 Identificación basado en el iris/retina 21

1.3.5 La firma 25

1.3.6 Geometría de la mano 26

1.4 Tecnologías más usadas en los sistemas penitenciarios 27

2 Capítulo 2: Módulo de Datos Personales e Identificación del SIGEP 29

2.1 Descripción de la solución propuesta para el sistema penitenciario venezolano 29

2.1.1 Rasgos físicos 30

2.1.2 Reseña decadactilar 31

2.1.3 Reseña fotográfica 33

2.1.4 Señas particulares 35

2.1.5 Identificación 36

2.2 Tecnología y medios 37

2.2.1 Solución biométrica de SAGEM 39

2.2.2 MSO SDK 39

2.2.3 AMK MSO300 ActiveX 41

2.2.4 XLS2 47

2.2.5 ActiveX de SAGEM 50

2.2.6 Dispositivos y medios físicos 51

2.2.7 Motivos de la selección 54
3 Capítulo 3: Integración de los dispositivos biométricos al SIGEP 56
3.1 Vista de arquitectura del módulo biométrico 56
3.2 ActiveX en la Web 59
3.3 Guía de Personalización XLS2 60
3.3.1 ActiveX y Ficheros de configuración 61
3.3.2 ActiveX reseña decadactilar 66
3.3.3 ActiveX para imagenes faciales 68
3.3.4 ActiveX para Cicatrices, Marcas y Tatuajes (SMT) 70
3.3.5 MorphoKit para la identificación. 71
3.4 Configuración del Componente XLS2 72
3.4.1 Instalación MSO 300 72
3.4.2 Instalación XLS2 73
3.5 Funciones y herramientas 73
3.5.1 Conversión de formato de imágenes 73
3.5.2 Configurar el ActiveX para Mozila firefox 74
4 Conclusiones 75
5 Recomendaciones 76
6 Referencias Bibliográficas 77
7 Anexos 79

TABLA DE IMÁGENES

Figura 1 Gráfica FAR-FRR 8
Figura 2 Esquema tecnologías biométricas 10
Figura 3 Representación del Iris 22
Figura 4 Geometría de la mano 26
Figura 5 Interfaz visual de Rasgos Físicos 31
Figura 6 Interfaz visual de Reseña Decadactilar 32
Figura 7 Interfaz visual de Reseña fotográfica 33
Figura 8 Interfaz visual de Nueva Reseña 34
Figura 9 Interfaz Visual de Histórico de Fotos 35
Figura 10 Interfaz visual de Señas particulares 36
Figura 11 Interfaz visual de Identificación 36
Figura 12 Diagrama de clases de MSO SDK 40
Figura 13 Diagrama de componentes ActiveX XLS2 47
Figura 14 MSO 300 52
Figura 16 Canon A 520 frontal 54
Figura 17 Canon A 520 parte posterior 54
Figura 18 Vista lógica de integración del ActiveX XLS2 57
Figura 19 Diagrama de despliegue 59
Figura 20 Carpeta SGM 60
Figura 21 ActiveX Capturar Resenna Decadactilar 67
Figura 22 ActiveX Four Facial 69
Figura 23 ActiveX Identificación 71
Figura 24 Carpeta MSO 300 73
Figura 25 Instalador MSO 300 83
Figura 26 83
Figura 27 84
Figura 28 84

Figura 29..... 85
Figura 30..... 86
Figura 31..... 86
Figura 32..... 87
Figura 33..... 87
Figura 34..... 88
Figura 35..... 88
Figura 36..... 89
Figura 37..... 89
Figura 38..... 90
Figura 39..... 90
Figura 40..... 91
Figura 41..... 91
Figura 42..... 92
Figura 43..... 93
Figura 44..... 93

Introducción

Las prisiones en todo el mundo han existido por siglos con la finalidad de mantener en áreas restringidas a personas para sancionarlas por hechos que cometieron. Se ha demostrado que las personas que pasan por estos recintos pueden educarse o convertirse en personas más antisociales. Por ello es que algunos gobiernos han tratado de que las prisiones ayuden a solucionar los males que la sociedad genera.

Los establecimientos penitenciarios venezolanos se caracterizan por el hacinamiento, inadecuadas instalaciones físicas, graves deficiencias en materia de servicios públicos y asistenciales, imperio de la violencia, extorsión, corrupción, inexistencia de inspección de los procesos, carencia de oportunidades y medios para la rehabilitación y reinserción de los privados(as) de libertad. En cuanto a los aspectos administrativos no se cuenta con una estructura organizativa integrada, se aprecia lentitud de los procesos administrativos y de gestión, las oficinas son inadecuadas, hay una ausencia de plataforma tecnológica, así como una inexistencia de enlaces con los entes externos que intervienen en los procesos.

Se puede agregar que el control de los individuos tiene escaso nivel de información con respecto al expediente judicial de cada individuo y carencia de identificación biométrica de los privados de libertad, lo que favorece prácticas reprobables y problemas en este recinto, como:

- La suplantación de identidad de individuos que se hacen pasar por otros para salir de los penales sin haber cumplido la condena.
- La ausencia de identificación; pues hay personas que no poseen cédula y otros que la cédula que poseen es falsa.
- Personas con varios nombres.
- Resulta difícil identificar individuos en caso que fallezca por cualquier razón dentro del centro penitenciario.

Esto en conjunto provoca que los individuos no cumplan cabalmente con la condena impuesta, que no se tenga un control exacto de la identidad de las personas que están sancionadas, que resulte complicado localizar a cualquier individuo después que es condenado y que no se tenga forma de validar que una persona es quien dice ser.

Por esto es que actualmente el Gobierno de Venezuela realiza esfuerzos por revertir la crítica e infrahumana situación que presentan sus establecimientos penitenciarios, como consecuencia del deterioro progresivo de su sistema penitenciario ha volcado también su esfuerzo en automatizar sus procesos por medio de sistemas informáticos. Por esto se crea el proyecto SIGEP "Sistema de Gestión Penitenciaria" en el marco de la colaboración Cuba – Venezuela. Con él se pretende desarrollar un sistema informático integral que permita gestionar la actividad penitenciaria, abarcando las áreas de control penal, clasificación y tratamiento, salud integral, custodia, control logístico, administración de la Dirección General y la gestión de sus unidades de apoyo así como el acompañamiento post penitenciario.

El Sistema de Gestión Penitenciaria (SIGEP) estará constituido por un conjunto de sistemas estructurados según las áreas que conforman la actividad penitenciaria: Sistema de Gestión de Privados de Libertad, Subsistema de Clasificación y Tratamiento, Sistema de Salud Integral, Sistema de Gestión de Establecimientos Penitenciarios, Sistemas de Gestión de las Unidades de Apoyo.

Sistema de Gestión de Privados de Libertad concebido para llevar el control del tránsito de los privados de libertad por el sistema penitenciario. Organizado en dos subsistemas: Control Penal, Clasificación y Tratamiento.

El Subsistema de Control Penal permitirá administrar los aspectos relacionados con la situación legal de los privados de libertad y el cumplimiento de la pena durante su tránsito por el sistema penitenciario. Este subsistema no tiene forma exacta de identificar a los individuos privados de libertad. Por lo que surge el ***problema científico*** ¿cómo mantener identificados a los individuos privados de libertad durante su tránsito por el Sistema Penitenciario Venezolano?

Para darle solución al problema planteado se toma como ***objeto de estudio*** la integración de las Tecnologías de Identificación Biométrica a aplicaciones informáticas y como ***campo de acción*** de la investigación es la integración de estas Tecnologías a aplicaciones desarrolladas sobre un entorno Java.

Como ***objetivo general*** se persigue: Integrar un módulo de identificación biométrica dentro del Subsistema de Datos Personales del SIGEP.

Para dar cumplimiento a este objetivo General se trazan los siguientes objetivos específicos:

- Estudiar y conceptualizar los elementos que intervienen en la identificación biométrica de personas.
- Estudiar las tecnologías y métodos de identificación de personas y seleccionar la tecnología a utilizar.
- Adaptar la tecnología seleccionada al marco de identificación en la captura de datos personales en el proyecto SIGEP.

Capítulo 1: Fundamentación Teórica

1.1 Identificación y reconocimiento de personas

Identificar a las personas ha sido crucial para la sociedad. En consecuencia, la identificación de personas es una parte integral en la vida cotidiana. Es usada en los sectores financieros, de salud, de transporte, de entretenimiento, cumplimiento de la ley, seguridad, control de acceso, control migratorio, gobierno y comunicación.

Independientemente del triste incremento de las actividades vandálicas todas las actividades del ser humano están basadas en reconocer, distinguir, identificar y ubicar a las personas. Incluso un principio que se utiliza para reconocer la salud mental de un individuo, es la capacidad de la persona de identificarse primero consigo misma y después con los demás (*La biometría: una realidad que ofrece seguridad* 2007).

Todos los días las personas se deben identificar para ingresar a las casas con una llave, para encender el auto, para prender un celular, para marcar el ingreso al centro de trabajo o para realizar transacciones financieras o trámites administrativos.

La utilización de diversas medidas de características físicas como técnica de verificación personal no es nueva. Ya en la antigua China, las impresiones dactilares de una persona eran utilizadas como firma personal y daban validez a documentos públicos y privados (REÍLLO and PUEBLA 2003). Por poner un ejemplo; a las huellas digitales, también se les menciona en la Biblia: “y puso un sello sobre su mano para memoria ante sus ojos” refiriéndose a ellas como una característica distintiva entre los seres humanos.

Recientemente han sido expuestas las tarjetas identificativas de los miles de soldados que cayeron en Normandía, y en los archivos de la Cruz Roja Internacional duermen millones de rostros sobados por las yemas de los dedos del investigador. Ninguno de nosotros reconocería hoy al “Héroe de Cascorro”, Eloy Gonzalo, último de Filipinas en la versión cinematográfica, si no hubiera posado ante la cámara de un galerista decimonónico apellidado Naranjo (FUENTES 2005).

Desde la antigüedad, el hombre ha tratado de controlar el acceso a determinados lugares, o a determinada información. Los sobres lacrados con el sello real, el conocimiento de un santo y seña, la utilización de un determinado uniforme, la posesión de una determinada llave (…) han permitido desde siempre el acceso a lugares restringidos. En la sociedad digital, se han sustituido los objetos anteriores por contraseñas, números PIN[1], certificados digitales, firmas digitales, (…) (RUIZ 2007).

Sin embargo estos objetos o datos pueden ser robados, falsificados, filtrados o deducidos. Es fácil conocer la contraseña de una persona o adivinar un número PIN. Para permitir autenticar a una persona, ya sea para acceder a un lugar físico, para efectuar una transacción bancaria o para realizar una compra se deben buscar métodos que no dependan de una "llave" determinada, sino que la propia persona sea la llave que le permita autenticarse. Es aquí donde entra la biometría (RUIZ 2007).

1.2 Características biométricas de los individuos que facilitan su identificación

Todos los individuos presentan características morfológicas que los distinguen. La forma de la cara, la geometría de las partes del cuerpo como las manos, los ojos, la huella digital, son algunos rasgos que los diferencian del resto de los seres humanos. A diario se identifican personas sin necesidad de darse cuenta. Ejemplificando, cuando se escucha una canción, el cerebro trata de probar si esa voz se parece a cualquiera de las conocidas y que han sido almacenadas a lo largo de la vida. Si el cerebro encuentra similitudes entonces se conoce a la persona que canta, sino se asume que es un desconocido. Del mismo modo los animales reconocen a otros animales, incluidos seres humanos, por características biométricas tales como olor, tacto, timbre de la voz, etcétera.

La biometría data sus inicios a finales del siglo XIX. En esas fechas, la Identificación Biométrica tenía un componente casi exclusivamente forense, y una aplicación fundamentalmente jurídico/policial asociada a técnicas de verificación personal a partir del estudio de las impresiones dactilares. A finales del siglo XX, los avances de los sistemas informáticos consiguen

[1] Un Número de Identificación Personal (PIN en Inglés) es un código numérico que es usado en ciertos sistemas para obtener acceso a algo, o identificarse.

que la Identificación Biométrica se expanda a otros entornos y, además, se exploren nuevas modalidades con las que realizar la Identificación.

Fue a finales de los años 90 cuando se empieza a ver la necesidad de crear interfaces comunes, así como formatos de datos conocidos. De ahí surgen iniciativas de carácter privado y sectorial, que impulsan determinadas tentativas de estándares de facto. Sin embargo, a consecuencia de los eventos del 11 de Septiembre de 2001, se empuja esa necesidad, y sobre todo, el hecho de que los acuerdos sean de índole mundial. (REÍLLO and PUEBLA 2003).

1.2.1 Concepto de biometría

La biometría es la disciplina que permite identificar a las personas basándose en características fisiológicas o de comportamiento. El término biometría viene del griego "bio" que significa vida y "metría" que significa medida o medición, de acuerdo al diccionario de la real academia de la lengua española Estudio mensurativo o estadístico de los fenómenos o procesos biológicos *(biometría 2007)*. En términos informáticos es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas.

La tecnología biométrica se basa en la comprobación científica de que existen elementos en las estructuras vivientes que son únicos e irrepetibles para cada individuo, de tal forma que, dichos elementos se constituyen en la única alternativa, técnicamente viable, para identificar positivamente a una persona sin necesidad de recurrir a firmas, contraseñas, códigos u otros que sean susceptibles de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos**.**

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad.

La identificación biométrica es utilizada para verificar la identidad de una persona midiendo digitalmente determinados rasgos de alguna característica física y comparando esas medidas con aquéllas de la misma persona guardadas en archivo en una base de datos o algunas veces en una tarjeta inteligente que lleva consigo la misma persona. Las características físicas

utilizadas son huellas digitales, huellas de la voz, geometría de la mano, el dibujo de las venas en la articulación de la mano y en la retina del ojo, la topografía del iris del ojo, rasgos faciales y la dinámica de escribir una firma e ingresarla en un teclado.

1.2.2 Rasgos característicos e indicadores biométricos

Cualquier proceso de identificación personal puede ser comprendido mediante un modelo simplificado. Este postula la existencia de tres indicadores de identidad que definen el proceso de identificación:

1. Conocimiento: la persona tiene conocimiento (un código)
2. Posesión: la persona posee un objeto (una tarjeta)
3. Característica: la persona tiene una característica que puede ser verificada (huellas, ADN, Voz)

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos:

1. Universalidad: cualquier persona posee esa característica
2. Unicidad: la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña
3. Permanencia: la característica no cambia en el tiempo
4. Cuantificación: la característica puede ser medida en forma cuantitativa

Los sistemas biométricos presentan también características como son: la necesidad de que las personas estén presentes en el lugar de la identificación, pueden o no requerir la colaboración del usuario e incluso pueden obviar la necesidad de que conozca la existencia de un sistema que lo está identificando. Es la herramienta de autenticación más segura y conveniente. No puede pedirse prestado, no puede robarse, olvidarse, y duplicarla es prácticamente imposible.

Los sistemas biométricos, presentan también dos conceptos importantes las tasas de falso rechazo FRR (False Reject Rate) y falsa aceptación FAR (False Acceptance Rate). Por

tasa de falso rechazo se entiende por la probabilidad de que un sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y tasa de falsa aceptación la probabilidad de que un sistema autentique correctamente a un usuario ilegítimo, evidentemente, un falso rechazo muy alto provoca descontento entre los usuarios del sistema, pero una elevada falsa aceptación provoca un problema grande de seguridad, pues estamos proporcionando acceso al sistema a un usuario ajeno a él, ver Figura 1.

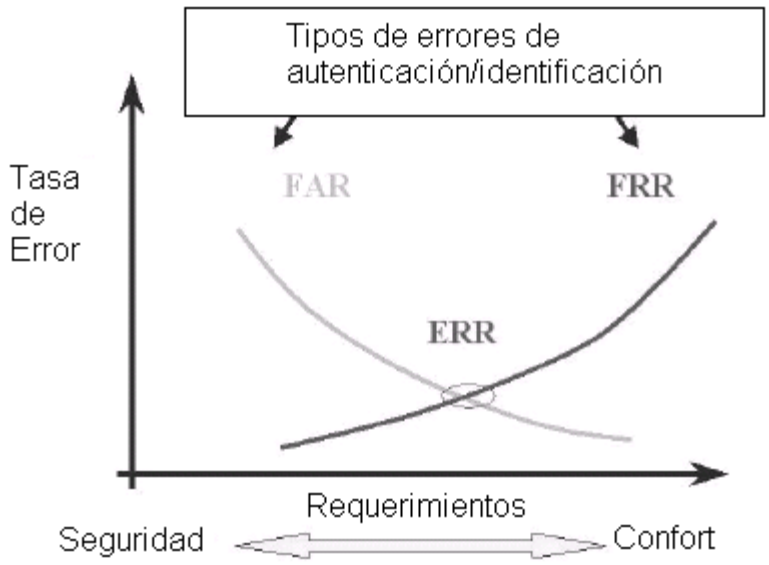

Figura 1 Gráfica FAR-FRR

ERR (Equal Error Rate): El FAR y el FRR responden a parámetros inversamente proporcionales, por tanto, variarán en función de las condiciones prefijadas por el programa de identificación biométrica. Así, si se debe utilizar el programa en un entorno de máxima seguridad, se intenta que el FAR sea el más pequeño posible, aunque esta acción signifique de forma implícita el incremento drástico del factor FRR. Se debe fijar un parámetro o umbral que permita igualar los dos factores, asegurando de esta manera el óptimo funcionamiento del sistema. Este umbral se denomina Equal Error Rate (GUTIÉRREZ), y es el que determinará, finalmente, el poder de identificación del sistema (DURÓ 2005).

La FAR debe ser lo suficientemente baja, en un rango que suele establecerse entre 0.0001 % y el 0.1%. Por ejemplo, en el 60% de las centrales nucleares de EE.UU. se emplean lectores de geometría de la mano con un FAR de 0,1 %. Hay que tomar en cuenta que la tasa real de entradas no autorizadas resulta del producto de que un sujeto no autorizado alcance el dispositivo de control durante el acceso (CORTÉS and PALACIOS).

La medición de las características corporales de las personas es conocida como biometría estática. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de Impresiones Dactilares, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen también, pero menos usadas, las técnicas biométricas basadas en forma de las orejas, temperatura corporal (termografía) y forma del cuerpo.

La medición de las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual.

De cada una de estas clasificaciones a medida que se conozca el cuerpo humano será capaz las tecnologías de incorporar parámetros cada vez más complejos y únicos que permitan identificar a los humanos.

A manera de resumen el siguiente esquema muestra la división de los sistemas biométricos.

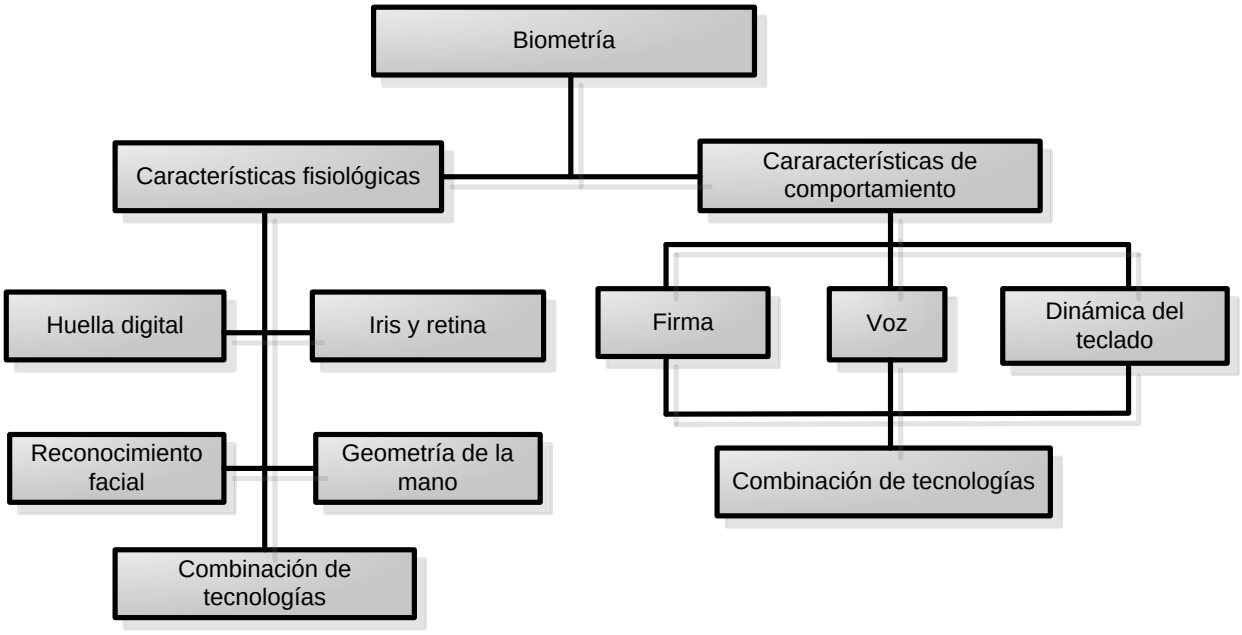

Figura 2 Esquema tecnologías biométricas

En la biometría hay tres términos de uso muy frecuente que son reconocimiento, verificación e identificación, cada uno de estos términos que a simple vista parecen muy similares, tienen significados muy diferentes.

Verificación/Autenticación: Es una tarea de los sistemas biométricos que busca confirmar la identidad de un individuo que la reclama comparando una muestra biométrica con la plantilla biométrica previamente ingresada al sistema. Durante la verificación; el sistema biométrico pregunta "¿es esta persona quien dice ser?" y compara este registro con el que está en un medio externo, por lo general una tarjeta lectora o simplemente una contraseña. La verificación es conocida como 1:1 (Uno a Uno)

Identificación: es una tarea donde los sistemas biométricos buscan determinar la identidad de un individuo. El dato biométrico es tomado y comparado contra las plantillas en la base de datos, la identificación puede ser cerrada (si se sabe que la persona existe en la base de datos) o abierta (si no se sabe con certeza si la persona existe en la base de datos), la identificación abierta también es llamada watchlist. La identificación implica el comparar una muestra contra una base de datos de muchas muestras registradas, mientras que la verificación implica el

comparar una muestra contra una base de datos que contiene una sola muestra. Durante la identificación, el sistema biométrico pregunta "¿quién es esta persona?" y establece si existe un expediente biométrico, y, si es así la identidad de la persona registrada que muestra es aceptada. La identificación es también llamada 1: N (Uno a muchos).

1.3 Tecnologías

Durante todo el siglo XX muchas empresas se dedicaron a desarrollar sistemas biométricos para garantizar su seguridad, así como también algunos departamentos de defensa de varios países. Restringido a través de su historia por su costo elevado, la identificación biométrica está experimentando ahora una creciente aceptación, no solo en aplicaciones de alta seguridad como bancos e instituciones gubernamentales, sino también en clubes de salud, control de clientes, acceso a oficinas y plantas. Los costos han sido reducidos a nivel razonable.

Hoy en día se cuenta con una variedad de equipos y sistemas capaces de identificar personas a partir de la información de alguna parte del cuerpo como las manos, la retina, el iris, los dedos, las huellas dactilares, la voz, la firma, incluso se está investigando en la posibilidad de crear un sistema basado en ADN.

El funcionamiento de los sistemas biométricos implica la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de las formas, la inteligencia artificial, complejos algoritmos matemáticos de aprendizaje, etcétera. El escáner de huellas y los equipos de medición de la geometría de la mano son los dispositivos más corrientemente usados.

Los sistemas biométricos se pueden dividir conceptualmente en cinco subsistemas: recolección de datos, transmisión, procesado de la señal, decisión y almacenamiento de datos.

Recolección de datos: Los sistemas biométricos comienzan con la medida de una característica del comportamiento o fisiología. La clave de todos los sistemas es: la hipótesis de las características biométricas son distintas entre los individuos y en cierto plazo repetible para el mismo individuo. Es decir, las características deben variar en gran magnitud entre individuos, pero deben variar muy poco para cada individuo de medida a medida. Por ende los sensores

deben ser estandarizados para asegurar que las características biométricas recogidas seas las mismas que las que recogería otro sistema para el mismo individuo.

Transmisión: Los sistemas biométricos recogen datos en una localización pero se almacenan y/o procesan en otras. Tales sistemas requieren la transmisión de datos. Si esto implica una gran cantidad de datos, la compresión es fundamental, a fin de requerir poco ancho de banda y poco espacio de almacenamiento. Los protocolos de la compresión y la transmisión deben ser estandarizados de modo que el usuario de datos pueda reconstruir (aunque con pérdida de la calidad) la imagen original. Los estándares para la compresión de la huella digital son WSQ[2], de las imágenes faciales JPEG[3], y de los datos de voz CELP[4].

Procesado de señal: Adquirida y transmitida una característica biométrica, se debe preparar para corresponderla con otra.

Decisión: La política de decisión dirige la búsqueda en la base de datos y determina la "coincidencia" o la "no – coincidencia". Este sistema toma en última instancia una decisión de aceptada o rechazada basado en las políticas del sistema.

Almacenamiento: Los requisitos de velocidad del sistema dictan que la base de datos esté repartida en subconjuntos pequeños o distribuida, tales que cualquier muestra necesite solo ser correspondida con los modelos salvados en una partición. Con esta estrategia se aumenta la velocidad del sistema.

1.3.1 Reconocimiento por Huellas Digitales

La identificación basada en la huella dactilar es uno de los métodos más antiguos de identificación biométrica. Su historia se remonta al año 2200 a.C. El uso de huellas dactilares como código personal tiene una larga tradición y ya era utilizado por los sirios, babilonios, chinos

[2] La especificación WSQ (Wavelet Scalar Quantization) fue diseñada específicamente para lograr altos grados de compresión de las imágenes de huellas dactilares, con una calidad superior. Con JPEG se alcanza una compresión de 1 a 6, mientras que con WSQ la relación es usualmente 1 a 15.
[3] Es un algoritmo diseñado para comprimir imágenes con 24 bits de profundidad o en escala de grises.
[4] Formato de compresión de audio a 19 kbits/segundo. Este formato requiere de mucho menos espacio de disco que el formato de compresión de audio de PCM, a 16 kHz. Del inglés Code Excited Linear Prediction.

y japoneses. La dactiloscopia (sinónimo de identificación de huellas dactilares no basada en ordenador) se usa en la investigación criminal desde 1897 (GRAEVENITZ).

La huella dactilar consta de crestas papilares (las líneas que cruzan en sentido ascendente la yema de los dedos) y surcos (los espacios entre las crestas) La combinación de crestas y surcos es única en cada individuo, aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímile o negativo de la huella.

En muchos países del mundo, las huellas digitales son reconocidas legalmente como sustituto de la firma escrita, indispensable para imponer obligación en un contrato o documento, en los casos en que la persona involucrada no pueda o no sepa firmar. Dentro de los diferentes métodos biométricos de identificación, la huella dactilar viene siendo el más aceptado y extendido por su alto nivel de fiabilidad y su excelente relación calidad precio.

Factores a tomar en cuenta para una buena captura

Verificar que la mano esté limpia, pues el aceite y suciedad de los dedos puede ensuciar el área de detección dejando una impresión fantasma llamada imagen latente.

Las autenticación por huellas digitales se toman de los dedos índices de ambas manos, tanto por la comodidad al capturarlas, como porque estos dedos están menos propensos que los pulgares a sufrir accidentes que dejen cicatriz. Porque para la solución de crímenes estos dedos, la

mayoría de las veces, son dejados en la escena del crimen. Aunque también se acepta la captura del dedo del medio y pulgar.

La arquitectura del sistema automático de reconocimiento de patrones de huellas dactilar consta, de tres partes:

1. Etapa de adquisición de datos: Adquisición mediante escáner, de la imagen de la huella dactilar.
2. Etapa de extracción de característica: a partir de la huella adquirida se extraen automáticamente la característica de la huella que conforman el patrón biométrico.
3. Etapa de comparación de patrones: El patrón de la huella que accede es comparado con el patrón registrado en la base de datos de usuarios.

Extracción de las características de la imagen

El objetivo de la etapa de procesado para la mejora de la imagen es el de proporcionar una imagen de la huella, con la calidad suficiente, para que el patrón biométrico generado por el extractor de características sea lo más fiable posible. Uno de los patrones de biométricos de huella dactilar más usados en los sistemas actuales, por su elevada fiabilidad, es aquel formado por el conjunto de puntos característicos que informa sobre la ubicación de las llamadas minucias de la imagen. Recibe el nombre de minucia cualquier punto de la imagen que indica que una determinada cresta presenta un final, un comienzo o una bifurcación. Una minucia estará determinada, por tanto, por sus coordenadas espaciales dentro de la imagen. Generalmente, los patrones biométricos de huella dactilar están constituidos por las coordenadas espaciales de cada minucia. Por orden podemos citar:

- **Huella:** se tiene una huella capturada
- **Normalización:** con la normalización se adapta el rango de variación de grises entre crestas y valles de la imagen a un rango deseado para facilitar el procesado de las siguientes etapas. El factor de normalización se calcula teniendo en cuenta la media y la varianza de luminancia en la imagen.

- **Campo de orientación:** la determinación de este campo permite conocer la orientación local de la cresta de la huella, necesaria para fijar los parámetros de los filtros adaptativos que se emplean en las etapas posteriores. Para ello se divide la imagen en bloques de 16x16 píxel y se calcula el gradiente en cada uno de ellos, en las coordenadas x e y. A partir del gradiente, el ángulo de orientación se determina mediante el algoritmo de ajuste de mínimo cuadrado. A veces en algunos bloques, la orientación del ángulo no se determina correctamente como consecuencia del ruido de fondo o daños en las crestas y los valles de la huella causada por defectos de la impresión en determinadas áreas de la imagen. Por tanto, para evitar esto se aplica un filtrado espacial de paso bajo para realinear todos los segmentos correctamente.
- **Elección de la zona de interés:** puesto que la imagen tiene un ruido de fondo, para evitar el cálculo de minucias fuera de área ocupada por la huella, se calcula la zona de interés definida por todos aquellos bloques en los que la varianza de los niveles de grises, en la dirección perpendicular de la cresta, es elevada. La zona ruidosa de la imagen viene dada por una varianza baja en todas las direcciones.
- **Extracción de las crestas:** La decisión de si un píxel pertenece o no a una cresta se consigue filtrando la imagen de la huella con dos mascaras adaptativas, capaces de aumentar la variación de nivel de gris en la dirección normal a la dirección de la cresta. La orientación de la máscara se adapta con cada bloque, teniendo en cuenta los ángulos obtenidos en el campo de orientación. Si el nivel de gris de un determinado píxel supera en un determinado umbral en las dos imágenes obtenidas tras el filtrado, se considera que dicho píxel pertenece a la cresta, obteniéndose así una imagen binaria de la huella. Después del filtrado de la imagen con estas mascaras los bordes de todas las crestas queden suavizados.
- **Perfilado de crestas:** con el fin de reducir el procesado de las siguientes etapas, se efectúa un nuevo filtrado para perfilar la cresta de las huellas y eliminar manchas en la imagen de la huella.
- **Adelgazamiento:** En esta etapa se aplican algoritmos consecutivos de adelgazamiento de imágenes con el fin de reducir el grosor de la cresta en la imagen binaria a un solo píxel. Estas operaciones son necesarias para obtener las minucias.

- **Eliminación de imperfecciones:** tras el adelgazamiento, dependiendo de la calidad de la imagen, se manifiesta en mayor o menor grado, las imperfecciones de la huella original, como puede ser las roturas de crestas y la aparición de crestas espurias y huecos. Se aplica, por tanto, un algoritmo de eliminación de todas las líneas que no son crestas, y de conexión de todas las crestas rotas.
- **Extracción de minucias:** finalmente, se extraen los puntos característicos que constituyen el patrón biométrico de la huella. Para ello, se determina si cada píxel de la imagen adelgazada pertenece o no a una cresta, en caso de que sea así, si pertenece a una bifurcación o a un principio o final de la cresta. El patrón biométrico resultante de este proceso contiene, típicamente, entre 80 y 90 puntos característicos, para el caso de la huella de tinta; y entre 30 y 45 puntos, para el caso de huellas adquiridas con escáner capacitivo.
- **Patrón de minucias:** reconocido en los sistemas como PK es el vector característico de la información de la huella. A partir de este es que se determinan en el AFIS la identificación, autenticación y validación de individuos.

Ventajas de la captura biométrica por huella

- Se ha demostrado la in varianza esencial de las huellas dactilares a lo largo de la vida de un individuo.
- Alta unicidad. Existe abundante evidencia que demuestra la extrema improbabilidad de que huellas de dedos distintos sean idénticas.
- Buenas prestaciones. Existen algoritmos eficientes de comparación de huellas. La información básica de las minucias puede almacenarse en poco espacio.
- Alta aceptabilidad. Aunque cabe significar que en casos esporádicos puede asociarse a criminalidad o invasión de la intimidad.

Desventaja de la captura biométrica por huella

- La adquisición de una buena impresión dactilar siempre se haya sujeta a la presencia de suciedad, cicatrices, heridas, etcétera. Así como muchos usuarios no saben poner el dedo correctamente en el lector.

1.3.2 Reconocimiento facial

De todos los rasgos anatómicos, el rostro es el elemento que con más frecuencia utilizamos los seres humanos para identificar a otro individuo. Para ello, el cerebro comienza por establecer los aspectos físicos de una cara, a continuación determina si estas facciones son conocidas o no y, por último, procede a otorgar un nombre a lo que ve.

En 1854 Ernest Lacan propuso la creación de un servicio fotográfico policial que resultó “práctico” en la identificación de involucrados en la Comuna de París (1871), pero que no fue establecido oficialmente hasta 1872. Hay que tener en cuenta que los delincuentes eran condenados no sólo por sus comportamientos al margen de la ley sino por las reincidencias en el delito, por lo que cambiaban habitualmente de nombre; incluso aquellos que eran buscados por delitos graves cometían fechorías menores para ser encarcelados y así camuflar su identidad al ingresar en prisión. La fotografía combatió en principio tales prácticas, aunque con el paso del tiempo los delincuentes modificaron su fisonomía para dificultar la identificación (FUENTES 2005).

Afirma Roland Barthes en La cámara lúcida que toda fotografía es un certificado de presencia (BARTHES 1994), por lo que el retrato fotográfico sería el certificado de presencia del individuo, el documento que legitima socialmente, la constatación incluso de nuestra existencia. Con esta premisa se explica que las tarjetas de identificación (documentos oficiales del país, pasaportes, bonos de transporte, carnés de prensa, tarjetas de crédito, etcétera.) incorporen el retrato fotográfico como documento que valida (revalida) la información contenida (relación texto-imagen), por lo que nuestra existencia depende, al menos parcialmente, de la similitud de rasgos entre el “yo presente” y el “yo representado” (FUENTES 2005).

Por otro lado Alphonse Bertillon estudió una nueva técnica en el que combinó fotografía y antropometría para obtener una identificación fiable y la localización inmediata de individuos. Presentó en 1880 los resultados y realizó una prueba con 700 reconocimientos que fueron correctos. El denominado Sistema Bertillon tuvo por objeto la identificación y clasificación de personas, especialmente de criminales, con dos premisas antropológicas fundamentales: las dimensiones de los huesos no cambian durante la edad adulta y son diferentes en cada persona. Tomaba fotografías de frente y perfil, así como detalles de la cabeza, cabello, nariz, orejas,

etcétera. Partiendo de la ficha fotográfica, la aplicación real del método permitió estructurar 75.000 fotografías de la prefectura de policía de París en unos 50 grupos, por lo que la búsqueda de datos era rápida y eficaz. En el año 1907 dio a conocer un método perfeccionado que se basó en una ingeniosa aplicación de las leyes de la perspectiva a la fotografía. Para ello creó un aparato especial con el que tomaba fotografías en varias escalas de objetos no mayores de 40 centímetros a una distancia media de dos metros de la cámara, de manera que la medida real del objeto podría conocerse partiendo de las medidas de las fotografías según un sistema de escalas.

Este proceso de identificación por el rostro puede resultar muy difícil para una máquina. Por eso, antes de desarrollar un sistema biométrico preciso, los científicos se han dedicado a analizar los procesos mentales de reconocimiento facial. De este modo han averiguado, por ejemplo, que existe una región en la base posterior del cerebro que responde preferentemente cuando se ven caras en contraste con la visión de otras partes de la anatomía o de objetos. También hay evidencias de que los procesos de interpretación de los gestos del rostro son independientes del proceso de identificación de caras, por lo que un buen sistema de reconocimiento facial debe ignorar la expresión facial.

No menos importante resulta saber que los humanos identificamos las caras de las personas de nuestra misma raza con mayor facilidad que las de personas de razas diferentes. Esto podría deberse a que el cerebro basa el reconocimiento de rostros en variaciones respecto a una cara "promedio" del entorno del sujeto.

Pese a las dificultades de imitar tan sofisticado proceso, los sistemas biométricos de reconocimiento facial empiezan a dar resultados. Aunque se trata de una tecnología no madura, en los últimos años han aumentado la inversión y las expectativas depositadas en ella.

Esta tecnología se ha popularizado recientemente por la gran cantidad de aplicaciones prácticas que ofrece, sin embargo se considera que existen distintos aspectos de la misma que deben madurar un poco más. Además, sus tasas de reconocimiento se ven limitados porque las imágenes de la cara no son patrones tan estables como el ADN o las huellas dactilares.

La cara de una misma persona puede resultar muy diferente dependiendo de la imagen que se tome. Las caras no son objetos rígidos, hay muchos factores como son expresiones faciales, los gestos, la iluminación, el maquillaje, la barba incluso con frecuencia la influencia del paso del tiempo.

El proceso de reconociendo de la cara consta principalmente de dos partes importante:

- Detección, localización de una cara humana en una imagen y aislándola de otros objetos en el marco.
- Reconocimiento, comparando la cara que es capturada con una base de datos de caras para encontrar una similitud.

Durante la detección, la combinación de los equipos y programas de computación aíslan los elementos faciales de una imagen y elimina la información extraña. El software examina la imagen en sus estructuras faciales típicas (tales como ojos y nariz), y una vez que los hayas encontrado, calcula el resto de la cara, entonces corta los detalles del fondo, dando como resultado una cara dentro de un marco rectangular llamado una máscara binaria.

La mayor dificultad para los sistemas de reconocimiento facial es que la cara de las personas cambia a través del tiempo. El sistema debe darse cuenta de esos cambios para poder ir actualizando los cambios.

Los sistemas de reconocimiento facial no solo trabajan con imágenes de rostro, algunos, incrementan su seguridad almacenando vistas frontales y laterales. Esto produce un mapa en 3D, que elimina la posibilidad de falla de seguridad utilizando fotos de legítimos usuarios. En estos casos, si el sistema no detecta que se trata de una imagen 3D rechaza el acceso.

La identificación por fotografía ha recobrado su significado tras los atentados terroristas de Nueva York (11 de septiembre de 2001) y Madrid (11 de marzo de 2004). La normativa de seguridad ha afectado directamente a instituciones públicas y a las compañías de transportes, en especial las aéreas, que obligan a presentar documentos acreditativos siempre con fotografía, tanto en vuelos internacionales como nacionales. En Estados Unidos se ha aplicado el sistema US-Visit, que verifica la identidad mediante una impresión electrónica de huellas dactilares y una fotografía

digital, decisión que afecta a millones de viajeros. Desde el 26 de octubre de 2003, todos los pasaportes deben llevar un dispositivo de lectura óptica y una fotografía identificativa

Las reacciones gubernamentales no se han hecho esperar. La primera prueba a gran escala de la biometría facial tendrá lugar en las fronteras estadounidenses, donde Estados Unidos exige el uso de pasaportes o visados biométricos. En España, el futuro DNI también incorporará un microchip con los datos personales en formato electrónico, una firma digital certificada y dos identificadores biométricos: la imagen facial y las huellas dactilares. Está previsto que entre en funcionamiento entre 2007 y 2008. Europa planea asimismo desarrollar nuevas tarjetas de crédito biométricas a través del Visa Information System *(VIS)* (*Reconocimiento Facial* 2007).

Desventajas

- Baja permanencia. El aspecto facial puede cambiar muy rápidamente debido al corte de pelo, barba, uso de gafas, etcétera.
- Baja unicidad. La capacidad de identificar a un individuo con respecto a otro es baja.
- Baja resistencia al engaño. El uso de medios como gafas, disfraces, peinado; pueden hacer que el sistema no funcione bien.

1.3.3 Sistemas de verificación de voz

La autenticación de Voz no está basada en el reconocimiento de voz como en la tecnología de autenticación por impresión de voz (voice- to-print authentication) dónde transforma la voz en texto. La biometría de Voz tiene un gran potencial porque no requiere de ningún nuevo hardware ya que la mayoría de las PCs contienen un micrófono. La idea central de los sistemas de verificación de voz es registrar el sonido emitido por un individuo e identificar sus patrones de timbre, intensidad y frecuencia. Sin embargo, la calidad pobre y ruido del ambiente pueden afectar la comprobación. Además, el procedimiento de la matriculación (enrollment) ha sido a menudo más complicado que con otras biometrías, llevando a la percepción de que la comprobación de voz no es amistosa para el usuario. Por consiguiente, el software de

autenticación de voz necesita mejoras. Algún día, la voz puede volverse una tecnología aditiva para la tecnología de huellas dactilares; porque muchas personas ven al escaneo de dedos como una forma de autenticación superior, se relegarán las biometrías de voz probablemente para reemplazar o reforzar los PIN´s, contraseñas, o nombres de cuenta.

Plantean algunos inconvenientes. Por un lado, su nivel de seguridad está aún por debajo de otros sistemas biométricos, ya que es sensible al ruido ambiental y puede verse influenciado, por ejemplo, por una simple congestión nasal. Además puede ser susceptible de engaño si se utilizan grabaciones, especialmente cuando se emplea una frase fija.

Otro problema del reconocimiento de voz es la inmunidad frente a replay attacks, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema.

Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o no; incluso el estado anímico de una persona varía su timbre...).

Desventajas

- Baja permanencia. Los parámetros básicos de la voz pueden alterarse fácilmente debido a muchos factores en periodos de tiempos muy cortos.
- Baja unicidad. La capacidad de identificar un individuo con respecto a otro es moderada, ya que un parecido de la voz no es raro.
- Baja resistencia al engaño. Una simple grabación puede engañar al sistema.

1.3.4 Identificación basado en el iris/retina

Aun pareciendo un sistema relativamente moderno, el uso del iris como medio de reconocimiento de personas nace a finales del siglo XIX como medio de identificación de criminales. Sin

embargo, no es hasta finales de los años 80 cuando se retoma el estudio del reconocimiento de iris como medio eficaz de identificación.

El reconocimiento del iris es considerado como uno de los medios más certeros y fiables dentro de la biometría.

El iris humano, es un órgano interior protegido por el ojo, es un anillo entre la pupila (generalmente, aparece en negro en una imagen) y la esclera (parte blanca que compone el ojo), se encuentra detrás de la cornea y el humor ácueo. El iris contiene gran cantidad de características muy precisas como, bastoncillos, coronas, pliegues, etcétera. Estas características visibles que son conocidas como *textura del iris*, son únicas y propias de cada individuo, ver Figura 3.

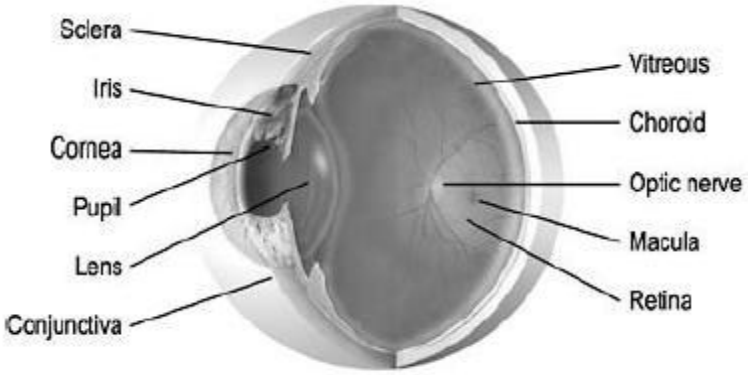

Figura 3 Representación del Iris

En el primer año de vida una manta células produce cambios en el color del iris, pero estudios clínicos muestran que el modelo del iris es estable durante toda la vida. La importancia del iris radica principalmente en el carácter único e individual para cada persona, siendo esto una de las principales ventajas de su uso en el campo de la seguridad empresarial y baluarte de su éxito y propagación por numerosos países en el mundo. Del mismo modo destaca también su carácter no intruso, entendido como la capacidad para capturarlos rasgos biométricos (la imagen del iris) sin necesidad de usar un medio que entre físicamente en contacto con el sujeto analizado.

El iris es tan único que no hay dos iris iguales, ni siquiera entre mellizos. En la actualidad, el convertir una imagen del iris en un código matemático es sumamente efectivo, ya que si dos o

más códigos llegan a coincidir en un porcentaje mayor al 75% la posibilidad que la similitud se encuentre en un error es de una entre 1.000 millones. Solamente en el iris existen 400 características distintas las cuales pueden ser cuantificadas y usadas para hacer posible la identificación.

Otra característica del ojo que se utiliza para reconocimiento es 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.

Hoy en día multitud de organizaciones utilizan el iris no solo en la investigación criminal, sino que también lo usan en el control a zonas restringidas, control de fronteras, identificación de empleados, seguridad financiera y en otros campos todavía hoy en desarrollo.

Todos los usos anteriormente mencionados podrían englobarse en los dos más importantes: la autenticación e identificación de personas. En la verificación las imágenes del iris se utilizan como medio de autentificación de la identidad de un individuo haciendo uso de la comparación “uno-a- uno” para determinar si la identidad reivindicada por la persona es verdadera o no.

Por otra parte, en la identificación, el iris es usado para reconocer a la persona buscando en una base de datos un patrón que le corresponda

Actualmente la investigación en el campo del reconocimiento del iris está desarrollando numerosas técnicas con el propósito de mejorar la eficiencia y la rapidez. John Daugman es el autor del algoritmo que actualmente usan la mayoría de sistemas, dada la eficiencia del 100% conseguida en las diferentes experimentaciones y pruebas. Es tal el éxito conseguido con este algoritmo, que dicho autor ha creado su propia compañía de sistemas de reconocimiento del iris.

Junto a la solución propuesta por Daugman, otros autores han creado diferentes algoritmos. Algunos algoritmos se basan en ligeras variaciones del propuesto por Daugman y otros proponen alternativas basándose en sistemas estadísticos, o mediante la utilización de patrones o plantillas. Las alternativas propuestas obtienen determinadas características del iris en su

totalidad, pero existen ciertas soluciones que sólo necesitan una pequeña porción del iris para la identificación. Puesto que la eficacia de los sistemas existentes es próxima al 100%, los avances que se realizan en la actualidad tratan de mejorar la eficiencia, así como abaratar los costes de los sistemas, ya que el uso de cámaras de alta resolución en el proceso de captura de la imagen incrementa notablemente el precio.

En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de 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 este 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. El sistema no es muy aceptado por los usuarios a pesar de que la tecnología en si trabaja bien. En tanto que esos dispositivos son bastante caros y usados solo en lugares de altísima seguridad

Los sistemas basados en el reconocimiento por el iris presentan dos métodos de adquisición; el primero llamado forma activa requiere que el usuario a identificar se mueva hacia atrás y adelante de manera tal que la cámara pueda ajustar el foco del iris del usuario. El segundo sistema pasivo es diferente ya que incorpora una serie de cámaras que localizan y enfocan el iris. Este método proporciona una mejor aceptación por parte de los usuarios finales.

Principales problemas de esta tecnología.

En primer lugar debemos destacar el número tan elevado de detalles que existen en el iris de una persona para un objetivo tan pequeño, de aproximadamente a 1 cm. de diámetro. Esto supone que el sistema se encargará de enfocar de manera adecuada el objetivo con el fin de capturar una imagen del iris nítida.

Otro problema al que nos enfrentamos también relacionado con la captura de la imagen, es el problema de la calidad, es decir, obtener una imagen del iris con una calidad aceptable para que pueda ser utilizada. Para solventar el problema de imágenes de calidad defectuosa se usa un descriptor de calidad que se encargará de descartar todas las imágenes que no superen un

determinado umbral. Además de recoger imágenes de calidad suficiente nuestro sistema deberá cerciorarse de que las imágenes pertenecen a personas vivas y no son una falsificación.

Una vez capturada la imagen el sistema se enfrentará a problemas relacionados con el tratamiento de la imagen, ya que esta deberá pasar por varias etapas antes de poder utilizarla de una manera adecuada. De este modo estos sistemas han de procesar la imagen (eliminar ruido, desigualdades de iluminación,...) para que posteriores funciones.

Finalmente se enfrenta con el problema de encontrar o diseñar sistema que cumpla con identificar al individuo de entre el conjunto de sujetos registrados, debido a que el precio y adaptación es alta.

1.3.5 La firma

La comprobación de la firma analiza la manera en que un usuario firma su nombre. Los rasgos del firmando, como la velocidad y presión, son tan importantes como la forma estética de la firma acabada. La comprobación de la firma disfruta una correlación con procesos existentes que otros sistemas biométricos no hacen. Las personas usan a las firmas como unos medios de comprobación de identidad para realizar transacciones, y la mayoría no vería nada raro que se parta de esto para abarcar la biometría. Los dispositivos de comprobación de firma son bastante exactos en el funcionamiento y obviamente se prestan a aplicaciones dónde una firma es un identificador aceptado.

La firma es candidato ideal a ser usado en el comercio como elemento de seguridad a la hora de efectuar transacciones (*Firma* 2007).

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se decremento su seguridad.

Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se le solicita tal firma, con un número limitado de intentos. La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

La desventaja es que relativamente pocas aplicaciones de firma han surgido comparado con otras metodologías de biometría.

1.3.6 Geometría de la mano

Los sistemas de autenticación basados en el análisis de la mano son sin dudas los más rápidos dentro de los biométricos; con una probabilidad de error aceptable en la mayoría de las ocasiones, en aproximadamente un segundo son capaces de determinar si un individuo es quien dice ser.

Uno de los elementos más importantes en este método es que son capaces de aprender; a la vez que autentican a los usuarios, actualizan su base de datos con los cambios que pueden producirse en la muestra (un pequeño adelgazamiento, el proceso de cicatrización de una herida) de esta forma son capaces de identificar a un usuario cuya se tomó hace años, pero que ha ido accediendo al sistema con regularidad, ver Figura 4.

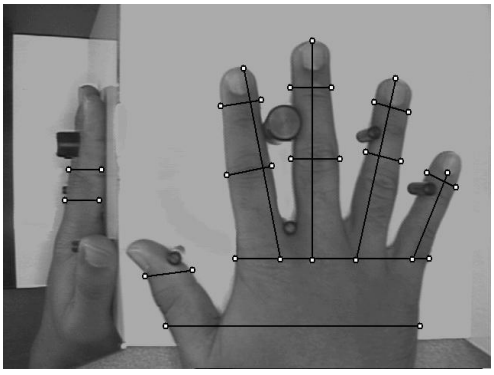

Figura 4 Geometría de la mano

El usuario pone su mano (normalmente la mano derecha; la máquina tiene un contorno de una mano derecha como guía para la colocación apropiada de la mano) en un lector que tiene cuatro palos tipo alfileres. Uno coloca su mano en el lector de tal manera que los alfileres paran el

movimiento delantero adicional de la mano. El método de autentificación mide el grosor y la longitud de los dedos y la distancia entre ellos. Crea un algoritmo único que se guarda normalmente en una banda magnética de una tarjeta tipo tarjeta de crédito.

Está siendo usado en los aeropuertos para controlar el acceso a las áreas propias de los empleados, para identificar frecuentes viajeros de negocios entre Estados Unidos y Canadá, así como a otros países extranjeros donde los ciudadanos de los Estados Unidos no necesitan visado. Los viajeros registran sus manos y les dan una tarjeta INSPASS para usarla durante los controles de seguridad. Por ejemplo, cada vez que pasajeros registrados pasan a través de la seguridad de los Estados Unidos en los aeropuertos importantes a y desde Canadá, insertan su tarjeta en el lector de tarjetas del kiosco (kiosko), ponen su mano en el lector de geometría de la mano, verifican su identidad, reciben una autorización de seguridad (en un papel), y continúan su camino. El proceso entero toma menos de 40 segundos.

La geometría de la mano tiene el beneficio de no ser un lector de huellas dactilares - no hay aura de criminalidad asociada con ello. Es exacto (la probabilidad de un duplicado de un algoritmo de la geometría de la mano es uno entre un millón), solamente menos que un lector de huellas dactilares. También requiere el uso de una interface activa. El usuario tiene que poner su mano directamente sobre el metal del lector.

1.4 Tecnologías más usadas en los sistemas penitenciarios

La biometría ha sido ampliamente usada en aplicaciones forenses como identificación de criminales y la seguridad en prisiones. Se han demostrado que las prisiones necesitan de un sistema de identificación robusto pero al mismo tiempo rápido. La necesidad de detectar a personas por órganos de seguridad nacional, o por la misma policía es en algunos momentos es de carácter vital. Resulta de una ayuda considerable los sistemas biométricos para lograr una identificación en las prisiones. Por otra parte no puede ser cambiada o falsificada, lo que hace de ellas sistemas confiables para estos recintos.

Los factores más importantes para elegir un sistema biométrico son las condiciones de uso, la cantidad de personas que usaran el sistema, las características fisiológicas de dichas personas,

la capacitación de las personas sobre el uso del sistema, el grado de cooperación al usarlo, el nivel de seguridad que se desea alcanzar y el tiempo de respuesta que debe tolerar el sistema. Por lo que debido a todos estos procesos la captura de huella digital, y el reconocimiento facial son los principales y que más cumplen con estos requisitos elementales.

Los sistemas de biometría dactilar destacan por su facilidad de uso, la buena aceptación que tienen por parte de los usuarios, por su facilidad de mantenimiento, y por las independencias de las condiciones de entorno (iluminación del ambiente, ruido del fondo, etcétera.)). Y sobre todo porque no necesita de la cooperación del individuo para ser capturada.

En el **Anexo 1.1** se puede presenciar algunas ventajas de los sistemas biométricos.

2 Capítulo 2: Módulo de Datos Personales e Identificación del SIGEP

2.1 Descripción de la solución propuesta para el sistema penitenciario venezolano

Las características de una prisión con respecto a otros sistemas hacen que se tomen en cuentan parámetros específicos, validaciones necesarias, suponer que los individuos a los que se captura la información no siempre están dispuestos a colaborar y no siempre dan la información con el detalle que se espera. Por ello lo importante es que los datos sean verídicos aunque los individuos hagan lo posible porque así no sea.

La solución que se desarrolle; debe validar que la información por la vía que la capture sea la correcta. Por lo que la propuesta de un sistema biométrico para que se solucionen gran parte de los problemas que presenta actualmente el sistema penitenciario venezolano, en la identificación de los individuos.

Por otra parte este paquete de desarrollo debe proporcionar una interface de programación que permita implementar un software con una interfaz de usuario de una forma fácil y rápida, ahorrando al programador tiempo y esfuerzos en el desarrollo de la aplicación. Buscando al mismo tiempo aceptación por parte del usuario, factibilidad, fiabilidad. Insertando junto a eso un sistema biométrico que incluya información gráfica y una descripción física de los individuos privados de libertad, algo que no se tenía organizado con el anterior procedimiento. Esa información gráfica incorporará, además de los datos dactilares, fotografías del individuo privado de libertad y sus posibles cicatrices o tatuajes, que se sumará a la información sobre su talla, color de ojos, de piel, su constitución física o el color de su pelo.

Con este registro exhaustivo de la población reclusa, la propuesta pretende dar un mayor control en las cárceles, que se ven afectadas por modalidades delictivas, cuyos miembros utilizan habitualmente multitud de identidades, que ahora serán despejadas de forma rápida tras contrastar sus huellas o imágenes del cuerpo con las del banco de datos. Así, cuando un individuo ingrese en prisión, y una vez que se tomen sus datos se comprobará primero si es quien dice ser, al mismo tiempo si ha estado o no encarcelado y otros datos de interés.

El subsistema dividido por pantallas que necesitan la captura de datos para identificar a individuos privados de libertad, resaltan:

Rasgos físicos: Para las características físicas y morfológicas como de la complexión, dimensiones, tallas del individuo.

Reseña decadactilar: Toda la información de la huella de los diez dedos. Para a partir de esta y con la información de un dedo, identificar a un individuo.

Reseña fotográfica: Permite captar 4 retrato faciales en pose derecha, izquierda, de frente y en mejor ángulo. En esta se sobresalta que se debe hacer un histórico de foto por el motivo de que las personas envejecen y se transforma su rostro.

Señas particulares: en el mismo se incluirá todas aquellas fotografías que me permitan identificar por tatuajes, marcas, cicatrices, heridas, etcétera. a un individuo.

2.1.1 Rasgos físicos

Permite describir por vía de las características de las personas como la forma de la boca, color de los ojos, color de la piel, tipo de pelo. Todas estas características unidas a las ya mencionadas huellas digitales, las imágenes fotográficas logran un sistema robusto de identificación. Aunque la deficiencia mayor radica que la decisión de un parámetro específico es absoluta del usuario del sistema, lo cual puede crear en algunos casos errores de apreciación que luego puedan repercutir. En caso de alguna duda que surja al observar algún rasgo de la Reseña Fotográfica en este punto de rasgo físico se logra limar.

Los Rasgos Físicos permiten tener un control para al mismo tiempo decidir del avituallamiento que se le entregará a un interno por los datos que aquí se recogen ya sea talla, complexión física del individuo, etcétera, ver Figura 5.

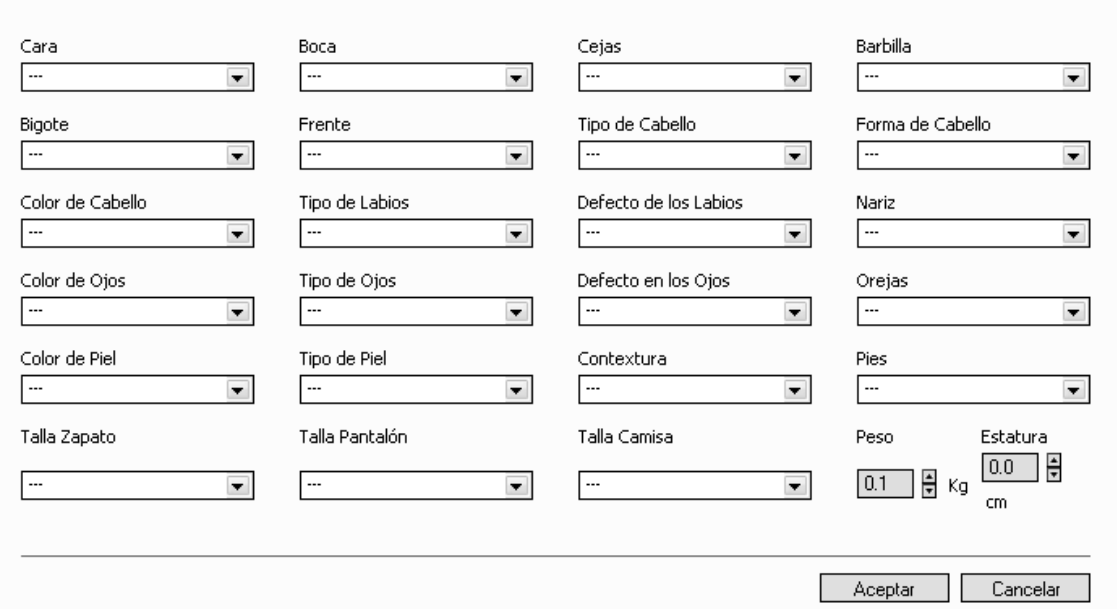

Figura 5 Interfaz visual de Rasgos Físicos

Para algunos valores de estos existen estandares, por lo que se puede escoger la opcion o si se tiene derechos de administración agregar uno nuevo.

2.1.2 Reseña decadactilar

Las huellas son únicas en cada individuo, se les considera, después del ADN el método más seguro para establecer una identidad ya que es poco probable que dos dedos tengan huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona.

En el momento en que un individuo privado de libertad necesita ser identificado, se le pide que coloque su dedo sobre un lector óptico, su huella dactilar es escaneada y analizada con el fin de extraer los elementos característicos y buscar su homóloga en la base de datos. Se ha comprobado, a raíz de estudios realizado por el Nacional Institute of Standards and Technology (NIST) en 2004, que el grado de precisión aumenta a medida que se incrementa el número de dedos cotejados.

En un sistema óptico, el dedo se coloca en una superficie de cristal, y una fuente de luz interna destaca los pliegues. El dispositivo de captura utiliza un sensor basado en CCD (Dispositivo acoplado de carga eléctrica). Se procesa la información por medio de componentes específicos

para cada productor de tecnologías biométricas y ya teniendo toda esta información ya una aplicación de identificación puede hacer uso. De ellas. Siempre se busca que el margen de error este entre 0,01% de fallas para que tenga fiabilidad.

Serán almacenadas las 10 huellas aunque con un dedo se realizará la identificación. Se tendrá la opción de actualizarlas huellas, por ejemplo si el individuo el día que se tomo la huella tenía un dedo vendado, puede después tomársele ésta.

Haciendo uso luego de patrones de comparación de huellas podemos llegar a la conclusión rápidamente y sin que el individuo tenga que saberlo validar la credibilidad de sus datos, si ya fue internado con anterioridad, si su identidad es verdadera así como otros requisitos indispensables para una eficiente identificación.

Descripción de la solución

Como se puede ver la secuencia de huellas se corresponde con el orden y posición de cada dedo, teniendo la posibilidad de ampliar la imagen para obtener una mejor visión por parte de la estructura de la huella, ver Figura 6.

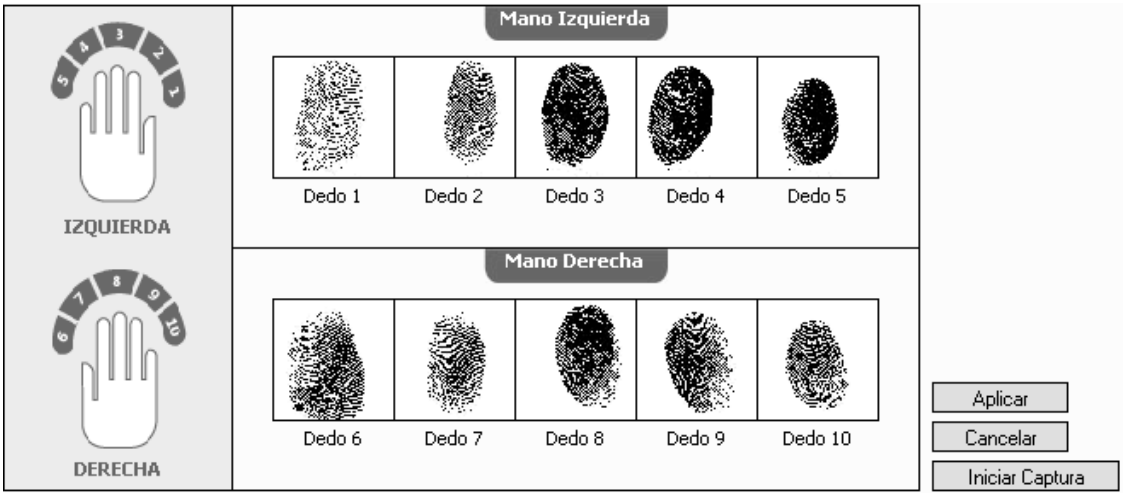

Figura 6 Interfaz visual de Reseña Decadactilar

El prototipo trata de darle una facilidad al usuario sin que tenga que llegar a términos informáticos, ni saber cómo se manejan los datos. Con la disposición de solo leer las funciones y

los mensajes de error. Se puede llegar a capturar una huella y solo guardarla cuando se esté seguro que la información que se implementa es válido para cada individuo.

2.1.3 Reseña fotográfica

El rostro las de personas son la forma más antigua que se conoce de la forma en que los animales se identifican, dígase con esto el hombre. Sin embargo, tiene sus limitaciones cuando existen personas con rostro similares por citar ejemplos gemelos, mellizos, una mala iluminación, un mal pose, un gesto; pueden hacer que se dificulte una buena identificación certera. Aunque esto no quita que un sistema biométrico basado en estas características no sea robusto.

Es importante resaltar que la reseña fotográfica no es en este sistema con el fin de identificación automatizada, sino más bien como forma de validar que las respuestas del sistema responden al rostro de una persona específica. Para cuando la información de un expediente se desee imprimir es bueno que lleve la foto del individuo al cual pertenece ya que esta le servirá al empleado tener una noción de si la persona es quien dice ser y que el sistema esta dando respuesta acertada, ver Figura 7.

Figura 7 Interfaz visual de Reseña fotográfica

Cuando se presiona el botón Nueva Reseña muestra la ventana de captura, ver Figura 8.

Figura 8 Interfaz visual de Nueva Reseña

Aunque la tecnología se enmarca en la captura de las imágenes por medio de un dispositivo como cámara fotográfica, se da la opción de que también se pueda acceder directamente a un directorio de la computador, permitiendo fotografías aun sin tener conectada una cámara.

2.1.4 Histórico de fotos

Tomando en cuenta que a diferencia de otras tecnologías como las huellas, los rasgos físicos; la reseña fotográfica son una característica que en las personas varía con el tiempo y analizando que un individuo en una prisión puede encontrarse por años, se hace necesario un histórico que se controle ese cambio.

En el mismo se llevará el control de todas las fotografías que se ha tomado el individuo privado de libertad por todo el sistema penal desde su primer acceso hasta la actualidad, ver Figura 9.

Figura 9 Interfaz Visual de Histórico de Fotos

2.1.5 Señas particulares

Las personas en el transcurso de su vida provocan condicional o incondicionalmente marcas en su cuerpo que algunas veces con una sola se puede determinar la identidad de una persona, mientras que integrándola con otras marcas del cuerpo pueden convertirse en un factor de identifican único por individuo. Tatuajes, heridas, cicatrices, quemaduras, verrugas, etcétera. La biometría se ocupa de cualquier detalle que permita identificar usando el cuerpo de las personas, por eso este factor no se pierde de vista.

Las señas particulares tienen la ventaja en comparación con la foto de retrato que no envejece junto con la persona por lo que una seña particular puede durar toda la vida a menos que una persona se dañe la piel o se realice algún tratamiento específico.

Los tatuajes convertidos para las personas como una moda, son en los centros penitenciarios algo común. En Japón a los 500 años d.C., el tatuaje ocupaba en los expresidiarios marcas en la frente y brazos, donde se podía leer la prisión donde habían estado, así pues se les despreciaba en comunidad, quitándole cualquier privilegio que en la comunidad pudiese dársele. Era uno de los peores castigos que se podían dar entonces. Actualmente tener frases, imágenes en el cuerpo que puede ocupar extremidades completas es moda. Por otro lado en las prisiones

también hay un gran número de personas con cicatrices en su cuerpo estos rasgos unidos componen un factor poderoso a la hora de identificar individuos.

Los tipos de señas particulares tomadas en cuentan son: tatuaje, cicatriz, mancha, cortada, quemado y verruga. Para estos se debe especificar en qué parte del cuerpo se encuentra así como una pequeña descripción del mismo, ver Figura 10.

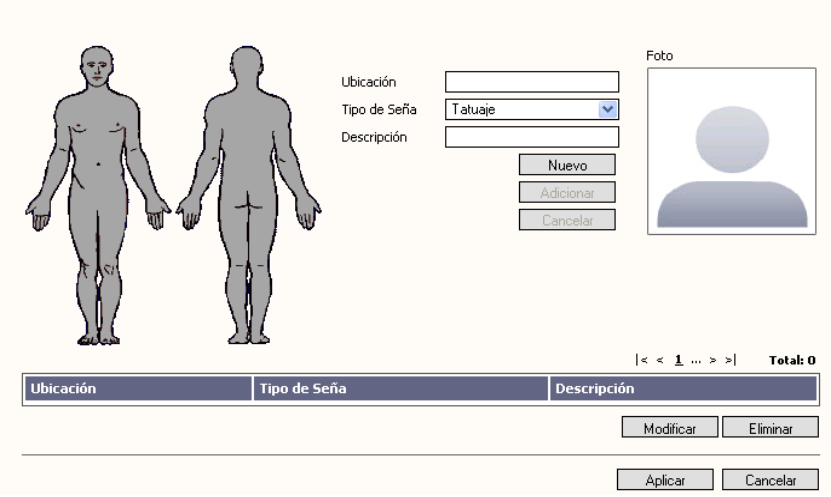

Figura 10 Interfaz visual de Señas particulares

2.1.6 Identificación

Aplicando los métodos de captura de imágenes, PK y vector de la huella se crea una base de datos que permite identificar a los internos, ver Figura 11.

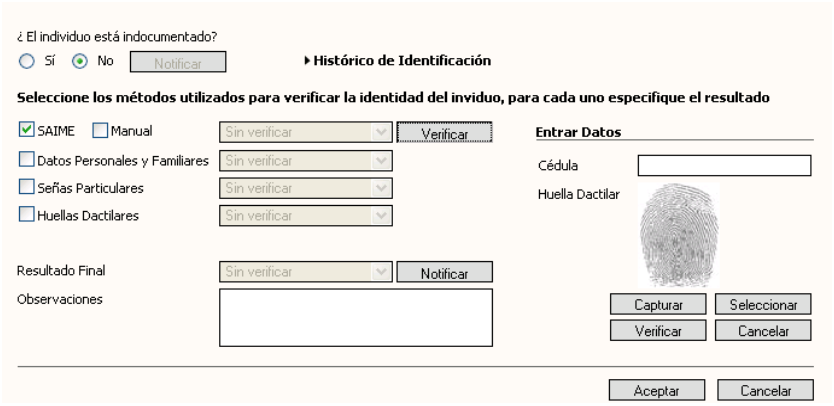

Figura 11 Interfaz visual de Identificación

2.2 Tecnología y medios

La tecnología que se usa para desarrollar el proyecto toma en cuenta parámetros tales como velocidad de respuesta, exactitud en la respuesta medida por la tasa de falso rechazo y falsa aceptación; también la aceptación por parte del usuario, la ventaja económica con respecto a otras aplicaciones, la adaptabilidad a la arquitectura propuesta.

Se podría decir que, en el diseño de un sistema, hay tres aspectos a tener en cuenta:

- la presentación de la información.
- la funcionalidad de la aplicación.
- la Arquitectura del Software (CASANOVAS 2004).

SAGEM (Sociedad de Aplicaciones Generales en Electricidad y Mecánica) es líder mundial en el campo de biometría con más del 49 % del mercado mundial. De SAGEM se puede resaltar, que por el gran mercado de identificación de huellas dactilares, con clientes que mucho pueden decir de la calidad del servicio como el FBI, INTERPOL, la policía francesa, alemana, inglesa e israelí, el servicio social de Nueva York, Filipinas, etcétera. Su aplicación se ha extendido a más de 80 países.

Como proveedor líder de tecnología de digitalización de huellas dactilares, ha desarrollado una nueva línea de dispositivos de identificación biométrica multipropósito, así como herramientas dirigidas a segmentos de mercado tan variado como aplicaciones forenses e institucionales (tarjetas de identificación, licencias de conducir, seguro social, etcétera.), así como aplicaciones comerciales (banco de comercio) e industriales (programas de fidelidad).

El Ministerio Interior de justicia de Venezuela es otro de los clientes de esta empresa, aplicando estos módulos en una serie de proyectos que actualmente se desarrollan en convenio con Cuba. Ya sea para la identificación, autenticación o servicios a otros proyectos. Esto representa una gran importancia por el hecho de que todos los convenios son firmados y asesorados por la parte venezolana, ya que el bloqueo impuesto a Cuba impide realizar algunos de estos convenios de nivel internacional formalizados.

Entre los productos que SAGEM ha lanzado al mercado podemos encontrar los productos biométricos para la captura e identificación de personas tales como:

- **MorphoTouch:** permite realizar un sinnúmero de transacciones desde un punto móvil, puede ser utilizado como punto de venta, identificador de personal, terminal para monederos electrónicos, pago de servicios, etcétera.
- **MorphoAccess:** La terminal de control de acceso permite la integración rápida a su sistema de control de acceso de un dispositivo biométrico de alta seguridad. Este dispositivo esta diseñado 100% para el mercado de control de acceso y asistencia e incluye el software de administración de huellas dactilares SAGEM. Puede ser manejado localmente o remoto. Con lector de tarjeta incluido.
- **MorphoPack:** es un dispositivo independiente de procesamiento de imágenes y comparación de huellas dactilares. Integra un sensor de huellas capacitivo en un lector compacto conectado a través de USB. Esto brinda una solución a bajo costo para requerimientos de identificación de huella dactilar 1 a 1 con alto grado de certidumbre.
- **MorphoKit:** brinda las herramientas necesarias para integrar a las aplicaciones la posibilidad de procesar huellas dactilares y realizar funciones de captura y comparación.

La solución propuesta es un módulo biométrico ofertado por SAGEM. Particularmente el modulo MorphoPack. Compuesto por el componente XLS2, drivers de dispositivos que se integraran en la solución, el Studio ILS2, ficheros de configuración, etcétera.

Este modulo biométrico permite capturar huellas dactilares, señas particulares (tatuajes, heridas, etcétera.), fotos en cuatro poses (de frente, derecha, izquierda, mejor Angulo.). Con un calidad validada por instituciones como el FBI, INTERPOL, etcétera. Este módulo ofrece una gama de funcionalidades para una rápida integración.

Con una serie de algoritmos que validan la calidad de la información. Con facilidades de integración al modulo de datos personales de SIGEP. Permite a medida que captura una imagen fotográfica realizar ajuste de centrado de la imagen ya sea automáticamente o por medio de que el usuario necesite modificarlo.

2.2.1 Solución biométrica de SAGEM

Por parte de este proveedor podemos encontrar tres productos como vías de solución el MSO SDK, AMK MSO300 ActiveX y el XLS2. Cada uno de estos módulos de desarrollo presenta diferencias palpables con respecto a los otros. Encontrar uno que se integre a la arquitectura del proyecto SIGEP buscando entre las funciones y al mismo tiempo que mas beneficien los requisitos captados.

2.2.2 MSO SDK

El MSO (Morpho Smart Optic) es una aplicación desarrollada por SAGEM la cual es usada para la autenticación e identificación de usuarios. Como lenguaje se emplea el Visual C++. Con la posibilidad de manejar huellas de adultos o juveniles. La autenticación puede ser realizada desde 1:1 hasta 1:20.

El MSO SDK puede ser usado con MSO 2XX, MSO 3XX, MSO 1300. Con posibilidad para conexión por el puerto serie RS232 [5] o por USB 1.1 o superior.

Para una mejor información al usuario este módulo permite una serie de mensajes asíncronos que muestran información de que debe hacer para lograr una captura exitosa, así como de posibles errores en la captura y por último si la huella fue tomada satisfactoriamente. Se encuentran ubicados en T_MORPHO_CALLBACK_COMMAND, dentro de la clase MORPHO_Types.h.

En la siguiente tabla se muestra la relación Identificación / autenticación de este módulo.

	Base de datos Local	Archivo PK
Huella en vivo	Autenticación e identificación	Autenticación
Archivo PK	Identificación	Autenticación

[5] Es una interfaz que designa una norma para el intercambio serie de datos binarios entre un DTE (Equipo terminal de datos) y un DCE (Data Communication Equipment, Equipo de terminación del circuito de datos)

A manera general se puede representar la arquitectura del MSO SDK como (ver la Figura 12):

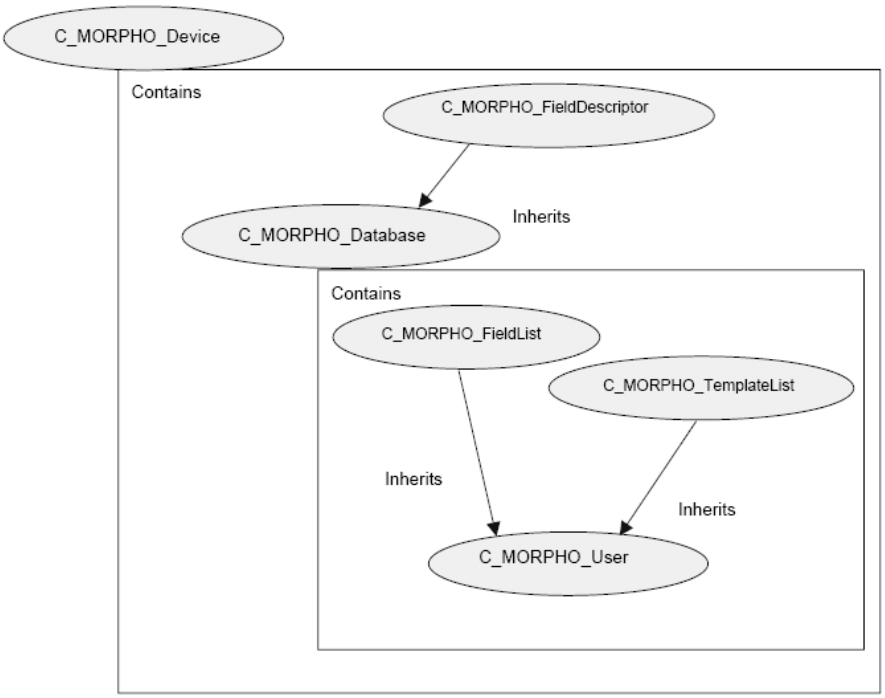

Figura 12 Diagrama de clases de MSO SDK

Funciones más importante de las clases antes mencionadas:

C_MORPHO_Device: esta asociada al dispositivo físico. El objetivo de esta es tener controlados a todos los dispositivos conectados, independiente de la base de datos.

InitUsbDevicesNameEnum()

GetUsbDevicesNameEnum()

OpenUsbDevice()

CloseDevice()

Capture()

GetDatabase()

Verify()

GetImage()

VerifyMatch()

C_MORPHO_Database: Asociada a la base de datos interna. El objetivo de esta clase es manejar la base de datos interna (crear, borrar, etcétera.). Esta clase hereda de C_MORPHO_FieldDescriptor. Al mismo incluye una o más instancias de C_MORPHO_User. Las instancias de esta clase deben ser asociadas con un objeto de dispositivo.

PutField()

DbCreate()

DbDelete()

GetUser()

Identify()

IdentifyMatch()

C_MORPHO_User: Clase asociada a un usuario. El objetivo de esta clase es manejar la información que tenga que ver con usuarios (insertar, autenticación de huellas, lectura de campos, etcétera.). Como un usuario es una lista de plantillas y una listas de campos de datos debe heredar de las clases C_MORPHO_FieldList and C_MORPHO_TemplateList. Las instancias de esta clase deben estar asociadas a una base de datos interna.

PutField()

Enroll()

C_MORPHO_FieldDescriptor: Clase que describe la estructura de los campos de de la base de datos interna.

C_MORPHO_FieldList: Clase que gestiona la lista de campos asociada a un usuario.

C_**MORPHO_TemplateList**: Gestiona la lista de plantillas.

C_MORPHO_UserList: Clase que gestiona la lista de usuarios.

C_MORPHO_Image: Clase que recibe y muestra una imagen de baja resolución adquirida en vivo.

2.2.3 AMK MSO300 ActiveX

Este módulo de SAGEM tiene una serie diferencias significativas con respecto a MSO SDK y es que no tiene base de datos interna. No puede ser usado con las versiones de MSO para puerto serie. No puede realizar identificación ya que no tiene base de datos interna con la cual

comprobar. Puede realizar autenticación pero solo con dos plantillas. Tiene poca gama de mensajes asíncronos, porque ya los trae predefinidos y en caso de cambio debe remitirse a una serie de ficheros y cambiarlo, mientras que en el MSO SDK solo eran mensajes mostrados a disposición del diseñador y analista.

El rango de FAR (Tasa de Falsa Aceptación) será de:

- 3000 para aplicaciones estándares (FAR < 0.1 %)
- 3500 para aplicaciones seguras (FAR < 0.01 %)
- 4000 para aplicaciones con alto nivel de seguridad (FAR < 0.001 %)

Se pueden citar algunas ventajas con respecto al MSO SDK tales como: solo se necesitan 3 clases y cerca de 10 funciones por clases. Las clases son IMKAquisition, IMKMinutiae, IMKImage. Puede ser programado usando lenguajes como HTML, Visual Basic y C++.

IMKAquisition: Para la captura de imágenes y plantillas de huellas

IMKMinutiae: Para el manejo de las plantillas de huellas.

IMKImage: Para el manejo de las imágenes de huellas (almacenamiento, conversión, etcétera).

Clase IMKAquisition

De la clase IMKAquisition se muestran funcionalidades biométricas como RunNoMatch, Run, Authentify. Parámetros de las funcionalidades biométricas como Status, matchingScore, TimeoutAcquisition, matchingThreshold, OnlyOneMatching. Parámetros del cuadro de dialogo como invetVideo, Halfsize, FingerCaption, UseConsolidation, WindowCaption, Languaje.

HRESULT Run (IMKImage *image, IMKMinutiae *pks, IMKMinutiae *refpks)

HRESULT invertVideo ([out, retval] short *pVal)

Fondo	Valor
Negro	True

Blanco	False

HRESULT UseConsolidation ([out, retval] short *pVal)

Modo de consolidación pVal

Activado	True
Desactivado	False

pResult Authentify (IMKMinutiae *pks, IMKMinutiae *refpks,[out, retval]short *pResult)

Como resultado esta función muestra:

Resultado pResult

Match	true
No Match	false

HRESULT WindowCaption ([in] BSTR newVal)

HRESULT RunNoMatch (IMKImage *image, IMKMinutiae *pks)

HRESULT matchingScore ([out, retval] short *pVal)

Valor status ([out, retval] short *pVal)

Resultado biométrico Valor

OK	0

CANCELLATION	1
NO MATCH	2
FAILURE	3
TIMEOUT	4

Clase IMKImage

Los objetos **IMKImage** contienen la imagen de la huella. Permitiendo manejar ya sea para salvar, mostrar. Imágenes de tipo RAW[6], BMP[7], JPG y WSQ así como la conversión entre los formatos previamente enumerados. Cada formato tiene un número que lo identifica.

Formato de imagen	Valor
RAW	0
BMP	1
JPG	2
WSQ	3

Algunas de las funciones que muestra esta clase son.

HRESULT Create (short sizeX, short sizeY, short numberOfBands)

[6] Es un formato de archivo digital de imágenes que contiene la totalidad de los datos de la imagen tal como ha sido captada por el sensor digital de la cámara fotográfica. El formato RAW no suele llevar aplicada compresión (sea con o sin pérdidas) como ocurre con el popular JPEG, aunque en algunos casos sí se emplea.
[7] Representan la sigla BitMaP (o también Bit Mapped Picture), o sea mapa de bits.

Dispositivo	sizeX x sizeY
MSO 300	416 x 416
MSO 1300 - CBM	256 x 400

Para el dispositivo MSO 300 el tamaño es 416 por 416, y el número de byte por pixel es de 1.

HRESULT Rotate90 ([in]short clockWise)

HRESULT SaveFile ([in]BSTR filePath,[in]long imageFormat)

Formato	imageFormat
Raw	0
Bmp	1
Jpg	2

HRESULT ReadFile ([in]BSTR filePath,[in]long sizeX,[in]long sizeY,[in]long nbBytePorPixel)

Casos	nbBytePorPixel
GrayScale	1
Color(RGB)	3

HRESULT GetImage ([in]long imageFormat,[out, retval] VARIANT *pVal)

HRESULT SetImage ([in]long imageFormat,[in]long sizeX,[in]long sizeY,[in]long nbBytePerPixel,[in] VARIANT newImage)

HRESULT CompressionFactor ([out, retval] long *pVal)

HRESULT CompressionFactor ([in] long newVal)

HRESULT numberOfBands ([out, retval] short *pVal)

Casos	pVal
GrayScale	1
Color(RGB)	3

En el caso de CompressionFactor ([in] long newVal) es válido para convertir imágenes a formato jpeg o wsq. Para formato jpeg, puede variar desde 1 hasta 100 (el valor por defecto es 80). Para el formato wsq, puede estar entre 20 y 1000 (por defecto toma 120)

Clase IMKMinutiae

Los objetos **IMKMinutiae** contienen la información de los puntos característicos de la huella. Para esta clase podemos encontrar una serie de funcionen tales como:

HRESULT Save (BSTR filename)

HRESULT SetRawData (int tipo, VARIANT *data)

Formato de la plantilla (HRESULT)	tipo
PK_COMP	1
PK_MAT	0

HRESULT rawDataAsVariant ([out, retval] VARIANT *pVal)

HRESULT Load (BSTR filename)

HRESULT size ([out, retval] short *pVal)

Formato de la plantilla (HRESULT)	pVal
PK_COMP	<= 170
PK_MAT	512

2.2.4 XLS2

El XLS2 de SAGEM es un producto que esta desarrollado para tecnologías Windows, y actualmente no se ha enfrascado en las soluciones Linux. Sin embargo brinda una serie de ventajas que son importantes, por citar algunas: este módulo biométrico, es capaz de reconocer dispositivos como escáner de impresión, cámaras fotográficas, escáner de huellas, etcétera. Por otro lado, con facilidades de adaptación a un entorno de desarrollo particular, le permite a los desarrolladores lograr configurar las interfaces de interacción por medio del Studio XLS2 un programa con controles estandarizados a esta interfaz, y por medio de ficheros con una conformación que se localizan en el directorio Booking.

Donde a manera de explicación la estructura del ActiveX se puede ver la Figura 13:

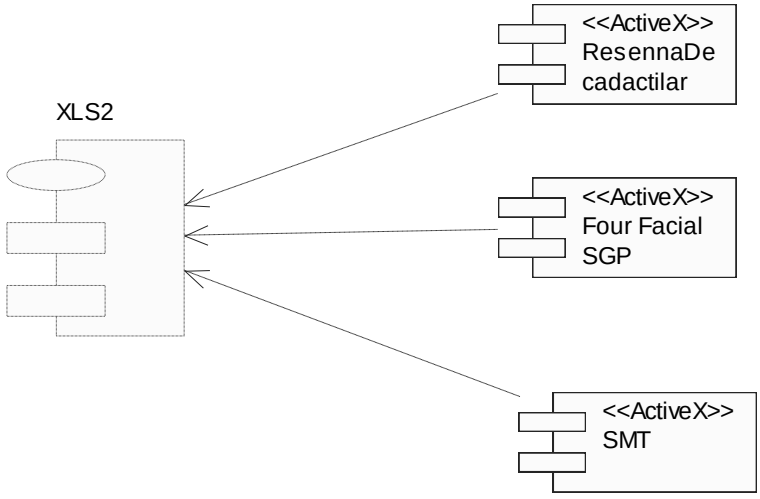

Figura 13 Diagrama de componentes ActiveX XLS2

Podemos destacar los tipos de registro:

- Ficha decadactilar: Un RecordType de ficha decadactilar corresponde a una lista de huellas que deben ser adquiridas. Podemos elegir solo algunos dedos; o todos los dedos y elegir la secuencia de adquisición, existen muchas oportunidades.
- Retrato fotográfico: Incluye AppearanceRecordType (imágenes faciales), SMTRecordType (cicatriz, señas y tatuaje) y EvidenceRecordType. Un RecordType de presencia corresponde a la lista que puede ser adquirido y el número total de páginas autorizadas. Podemos elegir de capturar solo algunos campos. El registro SMTRecordType es similar pero es utilizado para capturar y registrar cicatrices, señas y tatuajes mientras que captura otros tipos.

Las funciones más usadas son:

Ils2_StartTask() : permite lanzar la tarea de captura sobre el procedimiento previamente informado. Este método es llamado automáticamente durante la creación del modulo ILS2CaptureCtrl cuando los dos parámetros de configuración de idioma y de procedimiento son indicados.

Ils2_InitBloc() : permite solicitar una inicialización manual del bloque óptico.

BOOL Ils2_IsComplete() : este método da la posibilidad de saber si el procedimiento de captura se terminó correctamente, conforme a los parámetros de personalización y configuración establecidos.

short Ils2_GetStatus(short i__rank) : este método permite recuperar la decisión de SequenceCheck sobre la imagen correspondiente al rango « i__rank ». Esta decisión es el resultado preciso del control de secuencia y del control de calidad.El código de retorno de esta función, y la correspondiente descripción general de dicho código, se muestra en el siguiente

cuadro. La interpretación del código de retorno debe realizarse en función del tipo de dispositivo de captura empleado (es diferente para bopbopbop, MSO, etcétera.).

Códigos de retorno de Ils2_GetStatus y descripciones generales

Código de retorno de Ils2_GetStatus	Estado de la huella	Descripción general
-1	UNKNOWN	Desconocido
0	MISSING_ROLLED	Huella rolada faltante
1	MISSING_SLAP	Huella simultanea faltante
2	MATCH	Exitosa comparación entre huellas.
3	REVERSED_HANDS	Manos invertidas
4	REVERSED_FINGERS	Dedos invertidos
5	DOUBLED_FINGER	Dedo repetido
6	UNKNOWN_ROLLED	Huella rolada desconocida
7	PROBABLE_MATCH	Coincidencia probable
8	TOO_DARK	Muy oscuro
9	TOO_BRIGHT	Muy claro
10	BADLY_CONTRASTED	Mal contrastada
11	POORLY_ROLLED	Huella rolada pobremente
12	PRINT_OK	Huella bien
13	PALM_POOR_CAPTURE	Captura de palma pobre
14	PALM_POOR_CENTER_AREA	Área de centrado de palma pobre
15	POOR_QUALITY	Calidad pobre
16	POOR_MINUTAE	Minucia pobre
17	DECISION_UNDEFINED	Decisión indefinida
18	NOT_CHECKED	No verificado
19	BAD_NUMBER_OF_FINGER	Numero incorrecto de dedo
20	NOT_ACQUIRED	No adquirido
21	AMPUTATED	Amputado
22	BANDAGED	Vendado
23	DAMAGED	Dañado

VARIANT Ils2_GetImage(short i__rank, BSTR i__format, BOOL i__base64) : este método recupera la imagen de una huella en el rango « i__rank » en el formato « format » elegido dentro

de la lista (« RAW », « WSQ ») y codificada o no en base64 [8] según el valor del flag « base64 ». Devuelve NULL si ninguna imagen está presente en el rango indicado. Los datos son formateados dentro de un BSTR cuando están codificados en base64. Este BSTR se almacena en el atributo « bstrVal » del VARIANT de salida. En el caso que los datos no son codificados, éstas son almacenadas en el atributo « pcVal » del VARIANT de salida y el tamaño del buffer es definido en el atributo « decVal.Hi32 » del VARIANT de salida.

long Ils2_GetImageHeight(short i__rank) : este método recupera la altura de la imagen correspondiente al rango « i__rank ».

long Ils2_GetImageWidth(short i__rank) : este método muestra el largo de la imagen correspondiente al rango « i__rank ».

BOOL Ils2_IsBypassed (short i__rank) : este método muestra si la huella de rango « i__rank » ha sido salteado (bypass).

VARIANT Ils2_GetFeatureVector(short i__rank, BOOL i__base64) : este método captura la estructura FeatureVector asociada a la imagen de rango « i__rank ». Los datos se encuentran en un BSTR y codificada o no en base64 según el valor del flag « base64 ». Este BSTR es almacenado en el atributo « bstrVal » del VARIANT de salida.

VARIANT Ils2_GetAppearance(BSTR i__kind, BSTR i__id, BSTR i__format, BOOL i__base64) : este método permite recuperar las fotografías de los retratos en el formato « RAW » o « WSQ » y codificada o no en base64 según el valor del flag « base64 ».

VARIANT Ils2_GetSMT(BSTR i__kind, BSTR i__id, BSTR i__format, BOOL i__base64) : este método permite recuperar las fotografías de Cicatrices, Marcas y Tatuajes en formato (RAW) o (WSQ) y codificadas o no en base64 según el valor del flag (base64).

2.2.5 ActiveX de SAGEM

El ActiveX desarrollado por SAGEM permite crear un marco de trabajo con facilidades tanto para desarrolladores como para los usuarios finales. Con la ventaja de ser reconfigurable. Es conveniente por la posibilidad de adaptarlo a las funcionalidades de la aplicación.

[8] Es un sistema de numeración posicional que usa base64. Es la mayor potencia de dos que puede ser representada usando únicamente los caracteres imprimibles de ASCII.

No solo es usado para capturar la imagen y almacenarla, también permite validar y mostrar información de si la huella esta o no repetida, va mostrando información con mensajes asíncronos de ayuda para lograr una captura satisfactoria de la huella o la foto. Se valida todos los posibles errores y deficiencias de una mala captura. Puede ser reconfigurado para un lenguaje específico o para que la información que se maneja solo sea la deseada. Además de la captura de cada huella también el vector característico y las minucias. Con esta información es suficiente para identificar a una persona.

En el caso de las fotos retratos, se logra centrar la imagen, alinear los ojos, manejar el dispositivo desde la aplicación sin interactuar con él. Y en de la huella dice muestre el dedo a la derecha, a la izquierda, arriba, abajo, etcétera.

2.2.6 Dispositivos y medios físicos

Los dispositivos a usar serán:

Escáner de huellas MSO 300 de un dedo.

Cámara fotográfica Canon A 520

Trípode para soportar la cámara

Dongle, para validar la licencia del ActiveX

Cable de conexión a USB

Adaptador de corriente para cámara

Escáner de huellas de un dedo

El MorphoSmart™ Optic (MSO) es un escáner de huellas para captura de alta precisión, y excelente calidad de imagen adquirida para identificación, autenticación y registro. Dependiendo del modelo, el MorphoSmart óptico puede ser remoto y/o local. El remoto captura la imagen y la envía a un ordenador en el que este corriendo el MorphoSoft™ para plantillas de comparación. El tipo local captura, codifica, y descarta la imagen original y compara la imagen retenida en las plantillas con la de la base de datos en el terminal.

Se dispone del dispositivo MSO 300 para la captura de un dedo por el motivo que para realizar la identificación solo se necesita una huella. La conexión por medio de USB brinda posibilidades de plug and play. Aunque la integración con el ActiveX de SAGEM se realiza por medio de DLL que pueden ser actualizadas en caso que otro bloque óptico sea adquirido y se desee integrar al sistema, ver Figura 14.

Figura 14 MSO 300

Descripción técnica

Captura rápida de imágenes y de alta calidad.

Integración flexible para conexiones locales y remotas

Identificación 1: muchos y autenticación 1:1

Dos Leds [9] para ser usados como guía. (Para más información ver: Anexo Tabla 2.1).

Interfaz estándar USB 1.1

Peso 300 g

Dimisiones 80 x 92 x 57 mm

[9] Los led son bombillos indicadores de los dispositivos. Indican estados del funcionamiento.

Cámara digital

La Canon PowerShot A520 es una cámara digital extremadamente compacta de 4 megapixels y zoom óptico de 4 aumentos, que cuenta además con función de vídeo de alta calidad, flash avanzado incorporado y más de veinte modos de exposición diferentes, así como diversos accesorios adicionales. Usa tarjeta de memoria de tipo SD y un potente procesador de tipo DIGIC, el cual dota a la cámara de una rápida respuesta y gran versatilidad. Es posible adaptar objetivos de gran angular, primeros planos y teleobjetivo. Posee asimismo un menú muy bien organizado y funcional. La cámara fue presentada por Canon en febrero de 2005.

Un elemento innovador de especial relevancia en el Canon PowerShot A520 es el uso del potente procesador DIGIC, de reducidas dimensiones, el cual permite un consumo de energía muy eficiente y una rápida respuesta de la cámara. Como resultado, la cámara ofrece muy buenas prestaciones en situaciones de fotografía complejas, algo sin precedentes en una cámara compacta de estas características.

La Canon PowerShot A520 permite ajustar el punto focal mediante el uso de diversos tipos de objetivos, entre los que destacan de gran angular (Canon WC-DC52), primeros planos (Canon 250D) y teleobjetivo (Canon TC-52A), lo cual dota a la cámara de una gran versatilidad. De hecho, esta es una característica que diferencia claramente a esta cámara de otras de la competencia.

Características técnicas (ver Anexo Tabla 2)

Aunque ésta cámara presenta una tecnología sofisticada y las opciones del menú son varias, el ActiveX controla todos los parámetros reconfigurándolos según las necesidades del tipo de imagen que se desee captar, ya sea retrato, tatuajes, cicatrices, etcétera.

Figura 15 Canon A 520 frontal

Figura 16 Canon A 520 parte posterior

2.2.7 Motivos de la selección

El sistema penitenciario en Venezuela solo realizará identificación/autenticación sobre el sistema de Identificación Venezolana, este servicio es captado con el mismo producto por la otra parte por lo que la compatibilidad de formatos hace que la fiabilidad y seguridad de transmisión, respuesta sean superiores.

El dispositivos que se decide es el MSO 300 porque la autenticación que se llevará a cavo mediante una huella y un número de cédula, con un dispositivo de estas características se puede hacer cumpliendo con todos los requerimientos que se necesitan. Y por otro lado que el escáner de huellas de diez dedos de SAGEM actualiza la base de datos las huellas del AFIS y esto escapa del marco de responsabilidad de prisiones.

Con una razón de fuerza mayor se puede argumentar que SAGEM es el proveedor del AFIS civil y criminal del Ministerio del Interior y Justicia de Venezuela, por lo que ya se tienen convenios, regulaciones, etcétera. que hacen del producto se SAGEM un producto recomendado.

El proveedor SAGEM es líder mundial, por lo que la confiabilidad de su producto es fiable por criterios de otros usuarios. Ofrece alternativas de adaptación, ya sea por servicios web o por aplicaciones Windows. Además brinda documentación, capacitación del uso de la tecnología.

La Integración con otras soluciones es de vital importancia porque este módulo biométrico con los datos que reciba tendría toda la información necesaria, pero la autenticación que solo se realizará sobre El Sistema de Identificación Venezolana. También nuestro entorno de desarrollo es sobre tecnología java por lo que nos resulta provechoso para integrarlo en la Web.

Por otra parte se pueden mencionar algunas de las ventajas:

- Es universal pues todo el mundo tiene una cara y los dedos de las manos un alto por ciento
- Resulta fácil de obtener
- No es intrusiva

La facilidad de manejo del ActiveX es una de las ventajas referente a otros sistemas. Argumentando que el usuario no tendrá que tener conocimientos de dispositivos, ya que el sistema controla todo el proceso de captura de los datos. Al mismo tiempo es fácil de darle mantenimiento por la documentación que presenta así como por la facilidad de instalación.

3 Capítulo 3: Integración de los dispositivos biométricos al SIGEP

3.1 Vista de arquitectura del módulo biométrico

La arquitectura software trata el diseño e implementación de la estructura de alto nivel del software. Es el resultado de ensamblar un cierto número de elementos arquitectónicos para satisfacer la funcionalidad y ejecución de los requisitos del sistema; así como los requisitos no funcionales del mismo: fiabilidad, escalabilidad, portabilidad, disponibilidad, etcétera. Perry y Wolf **(1992)**

Muestra los componentes principales de diseño y sus relaciones de forma independiente de los detalles técnicos y de cómo la funcionalidad será implementada en la plataforma de ejecución. (LASSO 2007)

La arquitectura de SIGEP está dispuesta en tecnología Web basada en la plataforma Java o sea, un cliente con un servidor Web que accede a otro servidor que contendría los datos dentro de un gestor Oracle. Por lo tanto el ActiveX tendría que soportar toda esta arquitectura para que el sistema fuera robusto, ver Figura 18.

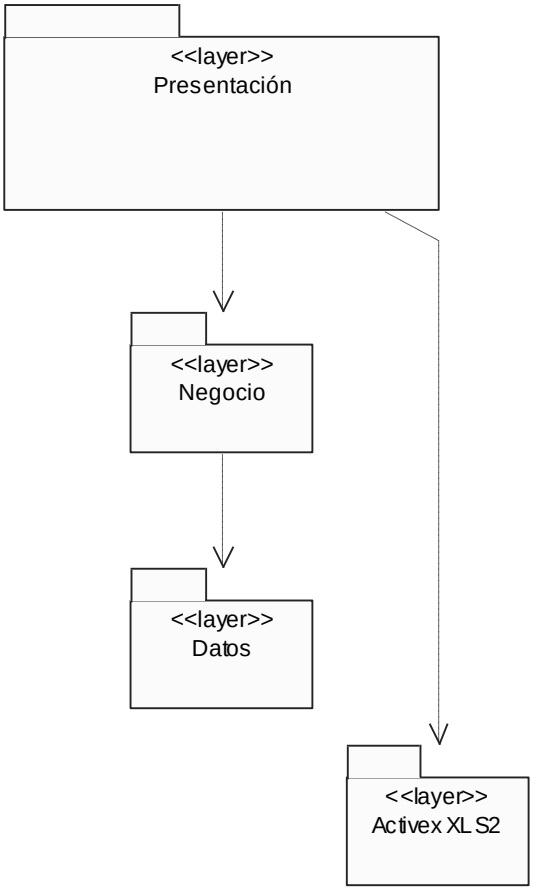

Figura 17 Vista lógica de integración del ActiveX XLS2

El inconveniente principal que se presenta es que el componente ActiveX es característico para sistemas Windows por lo que no es soportado por otros sistemas operativos ni por todos los browser.

Se definirá un sistema con arquitectura de tres capas, distribuidas cada una según las siguientes especificaciones:

- Cliente: Computador de tecnología Intel. La aplicación se ejecuta a través de un navegador de internet instalado sobre cualquier sistema operativo (se sugiere alguna distribución Linux y Windows XP solo para las estaciones de trabajo a las que se conectarán los dispositivos externos: en este caso el módulo biométrico con el escáner de

huellas, cámara digital). Máquina Virtual de Java, versión 1.5 para aplicaciones clientes que la necesiten.

- Servidor Web: En este servidor radica la lógica de negocio de la aplicación. Computador de tecnología Intel. Sistema operativo Linux RedHat 4.0, Advanced Server, para los servidores del centro de datos y alguna distribución de Linux para los servidores locales de los establecimientos penitenciarios. Servidor Web Apache Tomcat versión 5.x.x. Java Runtime Environment (JRE), versión 1.5.
- Servidor de Base de datos: Computador de tecnología Intel. Sistema operativo Linux RedHat 4.0, Advanced Server, para los servidores del centro de datos y alguna distribución de Linux para los servidores locales de los establecimientos penitenciarios. Servidor de base de datos Oracle 10g Standard Edition.

En el sistema por la necesidad de capturar las huellas e imágenes fotográficas y con ellas lograr una identificación de un interno se integró el XLS2 de SAGEM. Con este producto en SIGEP se logran los resultados esperados, con la desventaja que sólo es compatible para las tecnologías Windows y que para que esto funcione correctamente en Mozilla Firefox hay que reconfigurarle parámetros para que sean compatibles. Pero con la ventaja que es un módulo con prestaciones excelentes con pruebas ya realizadas en todo el mundo y con buena aceptación por parte de los usuarios que han usado el sistema.

Por eso se conformó para que sólo interactúe con la capa de interfaz como se muestra en figura 18. Con la ventaja de que es intrascendente el conocimiento por el ActiveX de la capa de acceso a datos y la capa de datos. Por otro lado que la ventaja de no estar unida permite que los dispositivos que se agreguen o cambien logren una mejor adaptación al entorno de desarrollo cumplimentado todas las funciones que espera el usuario de la aplicación.

Para el desarrollo del sistema se emplea una serie de dispositivos los cuales son integrados a una computadora por medio de Usb y puerto serie, a continuación se detalla el diagrama de despliegue que representa el módulo biométrico en la aplicación, ver Figura 19.

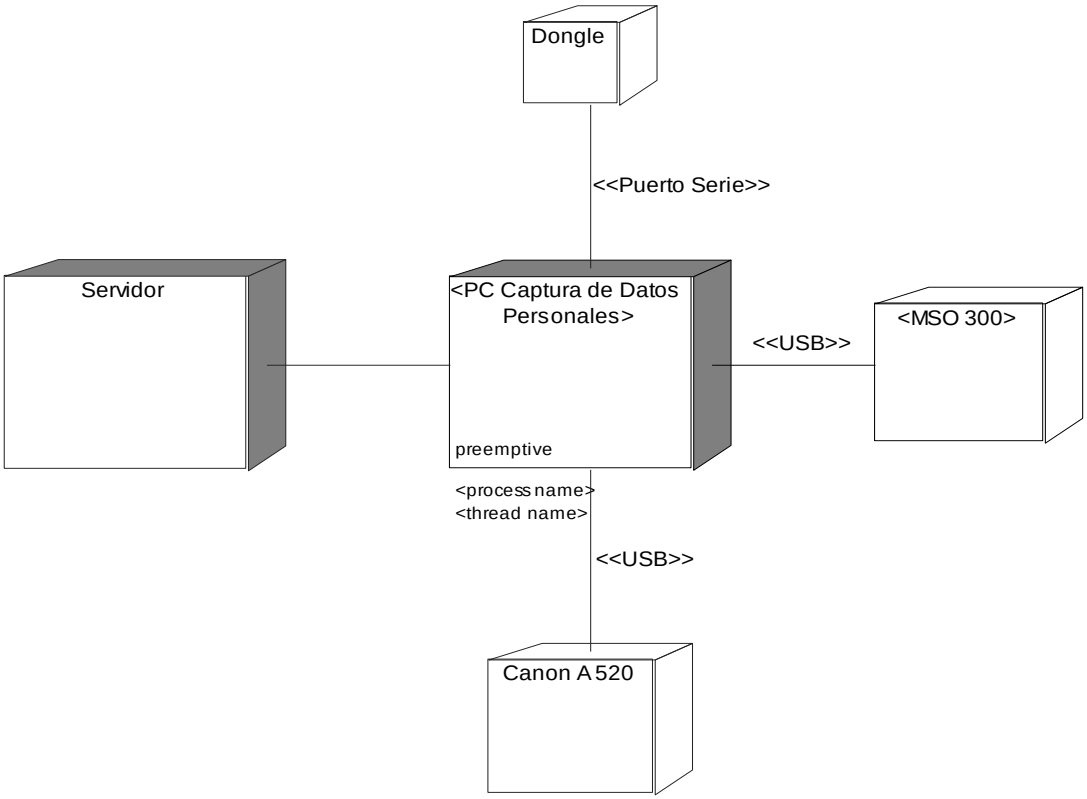

Figura 18 Diagrama de despliegue

3.2 ActiveX en la Web

El ActiveX está estructurado en una serie de ficheros de configuración que permiten ser modificados por medio del programa instalado Studio ILS2 en Booking para una mayor adaptación a las necesidades del proyecto.

Los ficheros de configuración se instalan por defecto junto al XLS2 en el directorio C:\Booking. Primero hay que tomar en cuenta que pueden ser varios los dispositivos y diferentes las funcionalidades que se desean de ellos. Por ejemplo, captura de huellas por medio del MSO 300, captura de imagen fotográfica por medio de la canon 520; por lo que se dividirá la explicación por funcionalidades como señas particulares, reseña fotográfica, reseña decadactilar e identificación.

Object ActiveX

Cada página web gestionará una funcionalidad específica ya sea Reseña decadactilar, Reseña fotográfica, Señas particulares, etcétera. Pero para un manejo eficiente de los componentes del

ActiveX este debe permitir a cada uno acceder a **SGM**. Por eso se debe especificar en cada página las funciones script que manejan los datos del ActiveX y un object que registra el ActiveX y lo ejecuta:

```
<OBJECT CLASSID="CLSID:BFCF8C39-A4D8-44C1-B2BF-0C1EFAC1E984"
        WIDTH=648 HEIGHT=336 ID="XLS2">
        <param name="Language" value="es_VE">
        </param>
        <param name="Procedure" value="huellas">
        </param>
</OBJECT>
```

En el object se le muestra “id” del ActiveX, el tamaño que tomará, y dos parámetros uno es el lenguaje y el otro el parámetro que dentro del fichero Procedures será reconocido, dejar claro que si este valor del Procedures no está bien identificado entonces provocará errores en el funcionamiento de la aplicación que es responsabilidad del desarrollador.

3.3 Guía de Personalización XLS2

A manera general accediendo al directorio C:\Booking se encuentra el fichero SGM. En SGM encontraremos Conf., en éste se muestran una serie de ficheros que permiten configurar la funcionalidad de los controles y los dispositivos desde el ActiveX, por otro lado tenemos ilog que es donde se encuentran todas las interfaces visuales con las cuales se interactúa. Hay que tomar en cuenta que cualquier modificación de parámetros mal realizada provocará un incorrecto funcionamiento en el XLS2 con errores que no se pueden capturar desde la aplicación, ver Figura 20.

Carpeta Conf

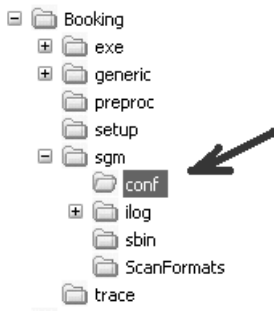

Figura 19 Carpeta SGM

Una advertencia significativa es que durante la personalización se debe modificar varios archivos de configuración que contienen bloques de alcance y parámetros.

Se debe ser cuidadoso porque:

- La eliminación inconsciente o consiente de un bloque de alcance o un parámetro puede causar la terminación sorpresiva de la aplicación de registro y errores progresivos de la aplicación.
- Un error de sintaxis durante la modificación de un archivo de configuración puede detener el inicio de la aplicación de registro.

Cuatro son los marcadores utilizados en la configuración. Estos marcadores identifican cuáles partes de los archivos deben ser modificados y cuáles no [**Personalización**], [**Parámetros**], [**Parámetros técnicos**], [**No cambiar]**.

3.3.1 ActiveX y Ficheros de configuración

Carpeta SGM

La carpeta de configuración SGM es un componente importante en el ActiveX. Por medio de ésta es que se modifican todos los parámetros, paneles, etcétera. Está dividido en dos Carpetas importantes (Conf, ilog), ver Figura 20.

- **Conf:** contiene todos los ficheros de configuración del xls2.
- **Ilog:** presenta todos los paneles de información, componentes visuales del ActiveX. Éstos serán modificados por el Studio ILS2.

Lista de los archivos de personalización y su contenido en **Conf**:

- Print_card_type.cfg : tipo de ficha de huella [No Cambiar]
- Signature.cfg : tipo de firma [Personalización]
- Mugshot.cfg : tipo de rostro [Personalización]
- Procedures.cfg : Procedimientos [Personalización]
- System.cfg : Definición de los caminos a los archivos [Parámetros]

- Gui.cfg : Definición de los accesos directos de teclado [Parámetros]
- Gui.cfg : FocusDraw [Parámetros]
- Gui.cfg : Menú [Parámetros]
- Gui.cfg : MessageBox [Parámetros]
- Capture.cfg : Captura [Personalización]
- Printing.cfg : FingerPrintBanner [Parámetros]

Print_card_type para la captura de huellas por el MSO 300

En el fichero …\conf\print_card_type.cfg se encuentra especificado las funcionalidades del panel para cada captura de huella dactilar.

La adaptación del MSO 300 para la captura de la huella digital desde el ActiveX tiene variantes de cantidad de dedos, daños en el dedo, etcétera. La adaptación estándar para cada usuario es un factor importante en el manejo del XLS2. Una captura de muchos datos o de pocos puede crear posteriormente errores o problemas de rendimiento a la hora de identificar o autenticar a una persona. Usualmente estos ficheros no deben modificarse pues han sido configurados por el proveedor de acuerdo a los requerimientos planteados por el usuario.

Cada dedo será identificado por número de dedo:

1: pulgar derecho

2: índice derecho

3: mayor derecho

4: anular derecho

5: meñique derecho

6: pulgar izquierdo

7: índice izquierdo

8: mayor izquierdo

9: anular izquierdo

10: meñique izquierdo

Se usa "**Only_fingers**":

```
scope PrintCardType
{
    list = ( "finger_thumbs_separate_sequence",
             "finger_rolled_thumbs_separate_sequence",
             "finger_thumbs_together_sequence",
             "palm_sequence",
             "common_finger_thumbs_separate_sequence_by_hand",
             "common_palm_sequence",
             "common_upperpalm_and_palm_sequence",
             "common_upperpalm_only",
             "common_bop_bop_bop_sequence",
             "bop_bop_bop_sequence",
             "scan_card",
             "only_fingers"
//           "left_hand_then_right_hand"
        );
```

Con la captura de los diez dedos (sólo se eligen los dedos al adicionar flat), el número que identifica el flat es el que corresponde a los dedos por el orden desde anular hasta meñique y de la mano derecha hasta la izquierda:

```
scope only_fingers
{
    capture_type = "onlyFingerCard";
    edition_panel = "CA-100-07SGP.ilv";
    images = (("FLAT","1"),
              ("FLAT","2"),
              ("FLAT","3"),
              ("FLAT","4"),
              ("FLAT","5"),
              ("FLAT","6"),
              ("FLAT","7"),
              ("FLAT","8"),
              ("FLAT","9"),
              ("FLAT","10"));
    allow_default_images_change = false;
    default_images = (("FLAT","1"),("FLAT","2"),("FLAT","3"),("FLAT","4"),("FLAT","5"),
                      ("FLAT","6"),("FLAT","7"),("FLAT","8"),("FLAT","9"),("FLAT","10"));
    mandatory = true;
};
```

Esta selección de dedos no deshabilita u oculta dedos visualmente, solo es para especificar que la información que se capturará es la de éstos y en este orden relacionado con la posición y la imagen. Para poder ocultar dedos o aumentar la cantidad es necesario hacerlo por medio del ILS2 Studio y la forma CA-100-07SGP.ilv que se explicará más adelante.

Se puede notar que el tipo de captura es "**OnlyFingerCard**", este parámetro es necesario para configurar el fichero procedures que se verá más adelante.

Mugshot fichero de configuración para la captura de fotos

Ya en este fichero se encuentra en…\conf\ mugshot.cfg. Debe tomar en cuenta que se necesitan varias formas de captura de fotos como son retrato facial en cuatro poses y para señas particulares como tatuajes, etcétera. Para cada uno de estos tipos de fotos se debe configurar diferentes parámetros.

Lo que más cabe resaltar en este aspecto es la necesidad de especificar correctamente la forma que será visualizada con cada funcionalidad, qué panel representa cada uno y la cantidad de imágenes.

Para identificar a las dos capturas de fotos, se nombra al retrato facial en cuatro poses como **FourFacial** y a las señas particulares **SMTRecordType** que identifica cicatrices (Scar), marcas (Mark) y tatuajes (Tattoo).

El bloque definirá cada apariencia con valores:

- Obligatorio: esta foto debe ser capturada o no
- allow_user_to_modify_photo_type: **true** el usuario podrá cambiar la pose de la foto a: FRONT, LEFT, RIGHT, ANGLED, NO_POSE. **false** el usuario no podrá modificar la pose de las foto.
- possible_angle_value: lista los posibles valores para el ángulo de la pose.
- pose: define la pose por defecto. Si allow_user_to_modify_photo_type es false, la pose será la pose especificada
- default_angle_value : cuando la pose es angular, el valor por defecto estará puesto a este valor

Procedures

En este fichero se crean los parámetros que se reconocerán desde el script del ActiveX. Ya éste es el acceso que tiene las formas visuales de llegar al ActiveX. Un parámetro puede presentar

más de una funcionalidad lo cual se mostrará en etiquetas diferentes, por ejemplo captura de huellas y fotos, para esto solo se agregará separado por comas dentro de componentes:

```
Scope compuesto
 {
  components = (
          ("OnlyFingerCard",  "Only_fingers"),
                  ("SMTRecord", "FourSMT")
   );
 };
```

Por poner un ejemplo el ActiveX que manejará la huella será identificado con el ID “huellas” para ello se debe especificar en el scope list que dará acceso a la Web. Además se le debe especificar a huella que función será la que ejecutará:

```
Scope huellas
 {
  components = (
    ("OnlyFingerCard",  "Only_fingers")
   );
 };
```

Para la foto se representa en el ActiveX y se referencia con el id “fotos”:

```
Scope fotos
 {
  components = (
    ("AppearanceRecord", "FourFacial")
   );
 };
```

Por último para las Señas particulares tendremos por identificados “SMT”:

```
scope SMT
 {
  components = (
    ("SMTRecord", "FourSMT")
   );
 };
```

3.3.2 ActiveX reseña decadactilar

El XLS2 permite capturar cada huella, dando facilidades y validaciones como dedo dañado, dedo repetido. Se denota el dedo que se captura para que el usuario tenga una guía. A partir de que se inicia la captura se escuchan dos pitidos de la bocina del sistema que determinan que el tiempo de captura máximo terminó. Esto logra que la huella esté el tiempo suficiente para una calidad aceptable. Al mismo tiempo en el área de la huella en vivo se va viendo la forma en que quedará la huella después de capturada.

Se debe estar consiente que el usuario del sistema que controle esta parte del proceso debe ser una persona confiable incorruptible y con conocimientos en esta tarea ya que de esta captura depende el buen funcionamiento del sistema. Incluso una mala captura puede provocar errores y elevar la tasa de falso rechazo o falsa aceptación por desconocimiento de un individuo por parte del sistema, ver Figura 21.

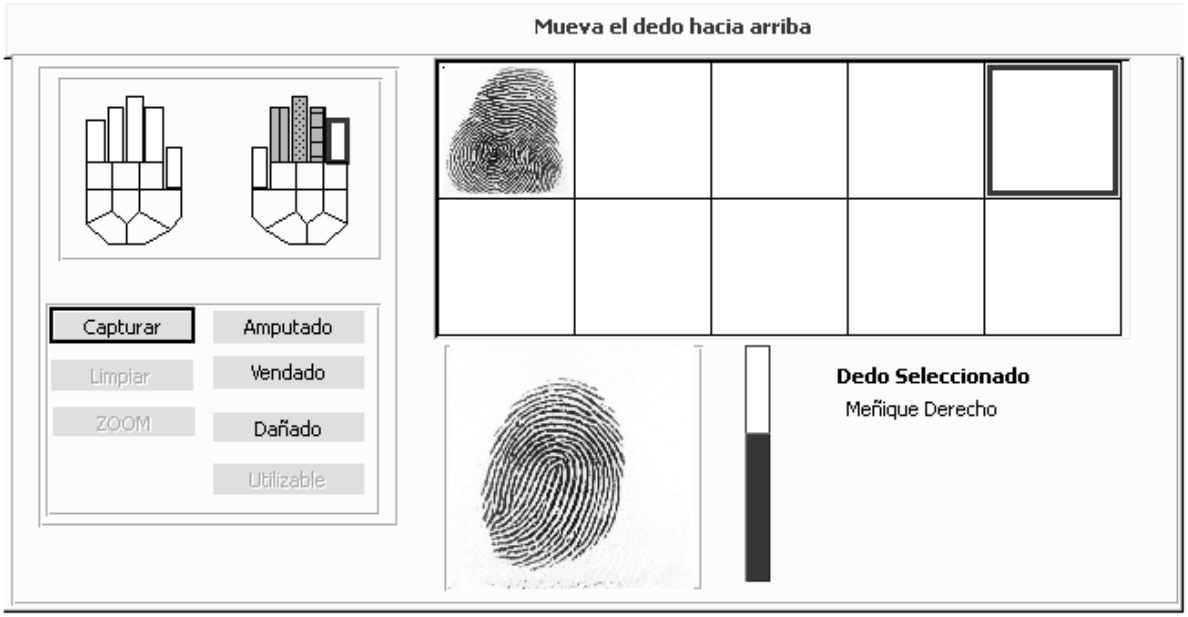

Figura 20 ActiveX Capturar Resenna Decadactilar

La función siguiente devuelve la imagen y el vector sobre el cual será sacado el PK.

```
function get_imageFeatureVector()
{

    for(l__count = 21; l__count < 31; l__count++)
    {
        l__width = XLS2.Ils2_GetImageWidth(l__count);
        l__height = XLS2.Ils2_GetImageHeight(l__count);
        if((l__width != 0)&&(l__height != 0))
        {
        l__image = XLS2.Ils2_GetImage(l__count,"RAW",1);
        XLS2.Ils2_SaveInFile("C:\\ActiveXFiles\\", l__count + ".raw") = l__image;
        l__featureVector = XLS2.Ils2_GetFeatureVector(l__count, 1);
        XLS2.Ils2_SaveInFile("C:\\ActiveXFiles\\", l__count + "_FV.b64") = l__featureVector;
        l__featureVector = XLS2.Ils2_GetFeatureVector(l__count, 0);
        XLS2.Ils2_SaveInFile("C:\\ActiveXFiles\\", l__count + "_FV.bin") = l__featureVector;
        }
    }
}
```

La siguiente función permite extraer el PK en C#.

```
public byte[] ExtraerDATOSPK( byte[] xDatosFV )
{
    try
    {
        if (!Inicializado)
            throw new Exception("Libreria Ecm.dll no presente !");

        byte[] _DATOSPK = new byte[512];
        System.Int16 res = MLEcm_extract_from_fv( xDatosFV, 1, _DATOSPK );

        if (res != 0x1001)
        {
            string msg = String.Format(
                "Resultado no esperado en la invocación al método MLEcm_extract_from_fv: {0}", res);
            throw new Exception( msg );
        }

        return _DATOSPK;
    }
    catch (Exception Ex)
    {
        throw new Exception("No pudo realizarse la extracción del PK a partir del FV.", Ex);
    }
}
```

3.3.3 ActiveX para imágenes faciales

El XLS2 permite capturar la foto, haciendo uso de un modo en vivo donde el usuario puede escoger el mejor momento para una captura satisfactoria. Con un control de modo ojos por el cual se alinea la imagen usando como guía los ojos. Presenta un área en vivo donde se verá el rostro de la persona y sirve como guía para hacer una captura correcta. La imagen capturada por su parte será mostrada en un retrato que se encuentra en la parte derecha. Ya en este retrato está la foto tal y como será guardada. Aquí el sistema debe haberle aplicado algoritmos para centrar los ojos y otros de adaptación de la luz, ver Figura 22.

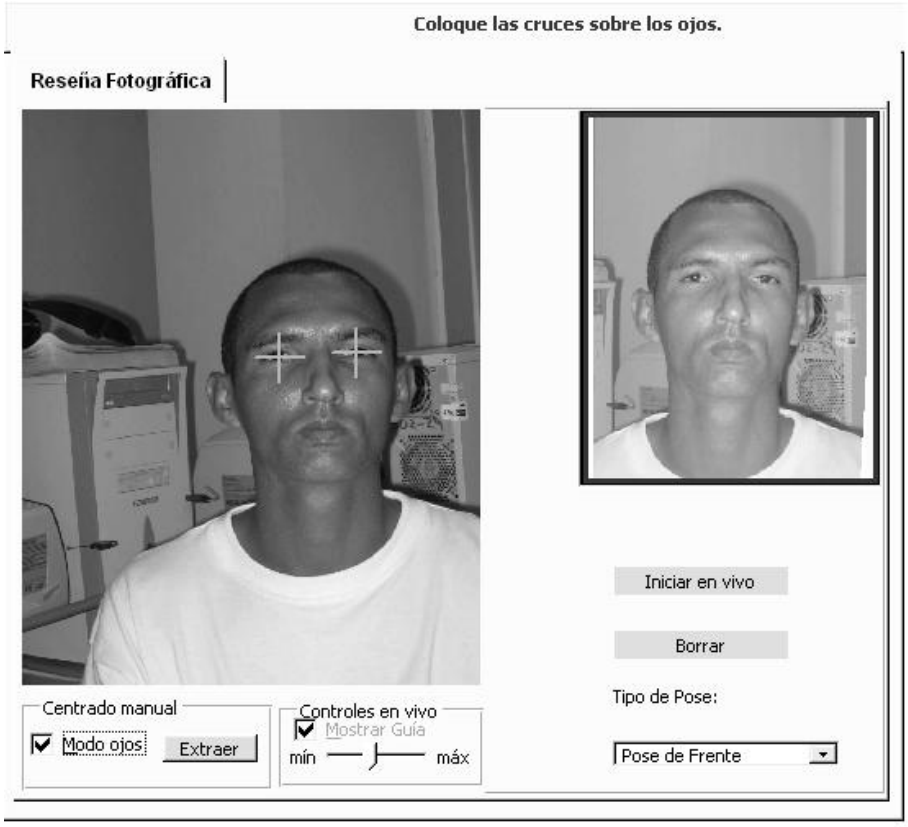

Figura 21 ActiveX Four Facial

Para obtener esta imagen la función que se debe usar es:

```
function get_appearance()
{

    l__kind = "APPEARANCE_1";
    l__id = "FACIAL_1";
    l__format = "JPG";
    l__base64 = 1;
    l__width = XLS2.Ils2_GetKindIdWidth(l__kind,l__id);
    l__height = XLS2.Ils2_GetKindIdHeight(l__kind,l__id);
    alert("Appearance size is " + l__width + " * " + l__height);
    if((l__width == 0)&&(l__height == 0))   {
        alert("Appearance size null, appearance won't be saved");
        return;
    }
    l__appearance = XLS2.Ils2_GetAppearance(l__kind,l__id,l__format,l__base64);
    alert(l__appearance);
    if(l__base64 == 1)
    {
        XLS2.Ils2_SaveInFile("C:\\ActiveXFiles\\", l__kind + "_" + l__id + "_64." + l__format) = l__appearance;
        alert("Image has been saved in C:\\ActiveXFiles\\" + l__kind + "_" + l__id + "_64." + l__format);
    }
    else
    {
        XLS2.Ils2_SaveInFile("C:\\", l__kind + "_" + l__id + "." + l__format) = l__appearance;
        alert("Image has been saved in C:\\ActiveXFiles\\" + l__kind + "_" + l__id + "." + l__format);
    }
}
```

3.3.4 ActiveX para Cicatrices, Marcas y Tatuajes (SMT)

Para la captura de marcas, cicatrices y tatuajes aunque tiene que ver con imágenes fotográficas necesita de otro control que realizará dicha tarea. Para ello se llama a la función get_smt().

```
function get_smt()
{
    l__kind = "SMT_RECORD_1"
    l__id = "SMT_1";
    l__format = prompt("Format (RAW/JPG)","RAW");
    l__base64 = prompt("Base64 encoded (0=no/1=yes)",0);

    l__width = XLS2.Ils2_GetKindIdWidth(l__kind,l__id);
    l__height = XLS2.Ils2_GetKindIdHeight(l__kind,l__id);

    alert("SMT size is " + l__width + " * " + l__height);
    if((l__width == 0)&&(l__height == 0))
    {
        alert("SMT size null, SMT won't be saved");
        return;
    }

    l__smt = XLS2.Ils2_GetSMT(l__kind,l__id,l__format,l__base64);
    if(l__base64 == 1)
    {
        XLS2.Ils2_SaveInFile("C:\\ActiveXFiles\\", l__kind + "_" + l__id + "_64." + l__format) = l__smt;
        alert("Image has been saved in C:\\ActiveXFiles\\" + l__kind + "_" + l__id + "_64." + l__format);
    }
    else
    {
        XLS2.Ils2_SaveInFile("C:\\ActiveXFiles\\", l__kind + "_" + l__id + "." + l__format) = l__smt;
        alert("Image has been saved in C:\\ActiveXFiles\\" + l__kind + "_" + l__id + "." + l__format);
    }
}
```

3.3.5 MorphoKit para la identificación.

La identificación de los individuos no es el fin de SIGEP, más bien se centra en el uso de un interfaz de servicios provistos por el Ministerio de Justicia y otros proyectos. Aunque no quita la posibilidad que se tenga, para de esta forma eliminar un tanto la transmisión en la red, así como la velocidad de respuesta. Por ello se usa el MorphoKit de SAGEM un módulo algo más pequeño y con menos funcionalidades, pero con la precondición de tener dos PKs para poder autenticar. Y la ventaja que tiene es que se puede integrar por medio de script.

Este pequeño módulo puede servir para realizar aplicaciones en lugares con difícil acceso a la red o nulo. Para con una base de datos interna o con transferencia por otra vía autenticar a los usuario, ver Figura 23.

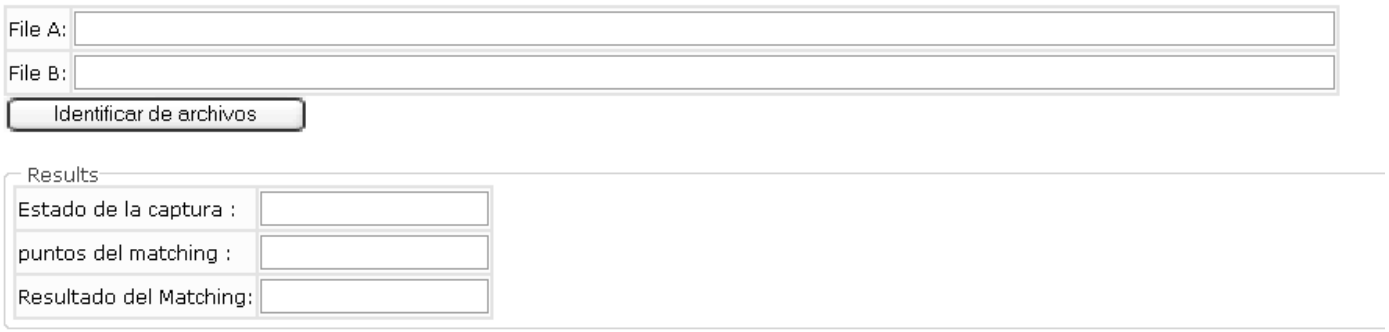

Figura 22 ActiveX Identificación

Para el uso de este módulo se debe especificar el path donde se encuentra el fichero con la información de los PKs, reconocible por el formato de SAGEM. Por otro lado se muestra el estado de la respuesta, los puntos que tienen de concordancia, así como el resultado de “Hit” en caso válido o “No Hit” en caso de error.

```
<SCRIPT language = "vbscript">

      Function AuthentifyFiles ()
        dim PK_A
        dim PK_B
        dim acquisition

        set acquisition = CreateObject ("AMK_MSO300.MKAcquisition")
        set PK_A        = CreateObject ("AMK_MSO300.MKMinutiae")
        set PK_B        = CreateObject ("AMK_MSO300.MKMinutiae")

        PK_A.Load (FileNameA.value)
        PK_B.Load (FileNameB.value)

        acquisition.Authentify PK_A, PK_B
        if acquisition.Status = 0 then
            MatchingResult.value = "Hit !"
        elseif acquisition.Status = 2 then
            MatchingResult.value = "No hit !"
        else
            MatchingResult.value = ""
        end if
        MatchingScore.value = acquisition.MatchingScore
        OperationStatus.value = acquisition.Status
    End Function

</SCRIPT>
```

3.4 Configuración del Componente XLS2

El proceso de configurar el XLS2 necesita una serie de pasos indispensables para una correcta puesta en funcionamiento. Como este ActiveX integra una serie de artefactos como dispositivos, ficheros de configuración, código script, etcétera; todo ello para poder funcionar íntegramente necesitan una minuciosa documentación que lo guía a una instalación correcta. Los pasos deben ser:

I. Instalar el driver del MSO 100

II. Instalar el XLS2

III. Sobrescribir el fichero SGM en el directorio Custo.

3.4.1 Instalación MSO 300

Instalar el MorphoSmart MSO 300 es muy simple, sólo requiere tener disponible un puerto Usb en la computadora.

Instalación de driver del MSO

En el directorio ...\MSO\mkit_3.10_protect\Launch.exe ver fig

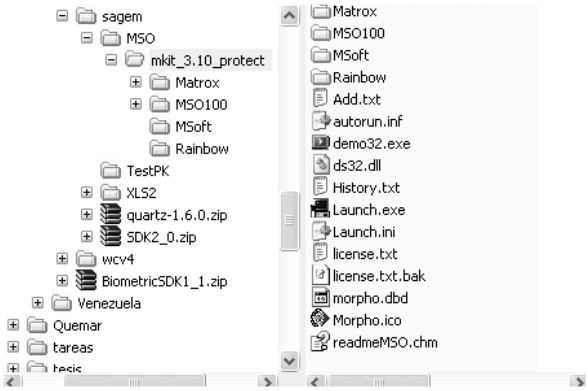

Figura 23 Carpeta MSO 300

Para que el sistema este correctamente instalado se pruebe con el MSO 300, si los leds están parpadeando en verde esta correctamente, en caso que parpadeen en rojo es que aun el sistema no lo reconoce. (Ver anexo 3.1)

3.4.2 Instalación XLS2

Para instalar completo el módulo ver los pasos a seguir en el Anexo 3.2 Guía de instalación del XLS2.

Después de terminar este paso el XLS2 está listo. Se puede utilizar la página Web para probar su funcionamiento en el módulo de Datos Personales de SIGEP.

3.5 Funciones y herramientas

Para un desarrollo de implementación se necesita integrar al proyecto una serie de funciones que servirán para manejar datos.

3.5.1 Conversión de formato de imágenes

El ActiveX maneja una serie de formatos de imágenes. Pero para poder trabajar con script es necesario que los datos en arreglos de bytes estén en formato base64, y para que una imagen sea mostrada en la Web debe estar en jpg o compatibles. Debido a esto hay que convertir de

arreglo de byte a jpg para poder mostrarlos. Por eso se usan estas dos funciones que permiten realizar esta tarea.

```
public class RawToJPGConvert {
    private int[] createPixels(int size) {
        int[] pixels = new int[size];
        Random r = new Random();
        for (int i = 0; i < size; ++i)
            pixels[i] = r.nextInt(0x1000000);
        return pixels;
    }

    public BufferedImage RawToJPG(byte[] bytes, int w, int h) {
        int[] pixels = createPixels(bytes.length);
        for (int i = 0; i < bytes.length; i++) {
            pixels[i] = bytes[i];
        }
        DataBuffer db = new DataBufferInt(pixels, w * h);
        WritableRaster raster = Raster.createPackedRaster(db, w, h, w,
                new int[] { 0xffffff, 0xffffff, 0xffffff }, null);
        ColorModel cm = new DirectColorModel(32, 0xffffff, 0xffffff, 0xffffff);
        return new BufferedImage(cm, raster, false, null);
    }
}
```

3.5.2 Configurar el ActiveX para Mozilla Firefox

Como medida prudencial que ha causado polémica, Firefox no incluye compatibilidad alguna con los sistemas ActiveX (soportados por Internet Explorer y extendidos en páginas Web interactivas). La mayoría de infecciones e intrusiones no permitidas al sistema Microsoft Windows son causadas por los controles ActiveX que permiten tener un control total sobre el sistema del visitante. Si bien esto puede ser una ventaja para ciertas aplicaciones, también es una vía libre, según Mozilla y los expertos en seguridad informática.

Por eso se debe seguir los siguientes pasos para solucionar este problema, instalando un pluging que permite el acceso de ActiveX desde Firefox.

- Instalar **MozillaControl1712.exe**
- Registrar la dll **regsvr32 mozctlx.dll**
- Arrastrar el pluging para el firefox **mozactivex-firefox (Custom).xpi**

Este punto es de vital importancia para el que la aplicación funcione. Si se toma en cuenta que el uso de un sistema desde tecnología Web es necesario que sea compatible con los dos browser mas usados en la actualidad digamos Mozilla firefox y Internet explorer.

4 Conclusiones

Las tecnologías biométricas son la solución para aplicaciones que desean identificar usuarios. Cumpliendo con los objetivos propuestos en el trabajo se llega a la conclusión que se logró integrar el módulo biométrico al módulo de datos personales del proyecto SIGEP. Identificando con ello a los individuos privados de libertad y con ello la satisfacción del usuario. Con esta solución se hará de las prisiones en Venezuela lugares más seguros.

Como tecnología biométrica se usó el ActiveX XLS2 del paquete MorphoPack de SAGEM.

5 Recomendaciones

Actualmente en Cuba no se tiene un sistema de identificación automatizado por medio de un módulo biométrico, por eso se recomienda que se integre a una aplicación una solución de software que permita identificar a los privados de libertad en el país. Por otro lado, en la Universidad se debe realizar estudios en las tecnologías biométricas para lograr crear componentes y que no sea necesario recorrer a empresas exteriores.

6 Referencias Bibliográficas

BARTHES, R. *La cámara lúcida*. 1994. pp. 421-423 p. ISBN-13: 9788475096216

biometría. Vigésima Segunda Edición. 2007. [Disponible en: http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA="biometría%20es%20el%20estudio%20mensurativo"

CASANOVAS, J. *Usabilidad y arquitectura del software*, 2004. [2007]. Disponible en: http://www.alzado.org/articulo.php?id_art=355

CORTÉS, J. C. P. and R. P. PALACIOS. *Sistema de seguridad basados características Biométricas*. *Instituto Tecnológico de Informática*.

DURÓ, V. E. *Evaluación de Sistemas de Reconocimiento Biométrico*, 2005.

Firma. 2007. [Disponible en: http://www.elvilmetal.com/empresas/biometria-para-acceder-muestre.php

FUENTES, J. M. S. V. B. F. La fotografía como documento de identidad, 2005, vol, 28: 189-195.

GRAEVENITZ, G. A. V. Tecnologías de identificación por huella dactilar.

GUTIÉRREZ, A. D. J. *Importancia de la documentación*. *Mygnet*, 2006.

La biometría: una realidad que ofrece seguridad. 2007. [Disponible en: http://www.imcyc.com/cyt/enero02/biometria.htm

LASSO, A. *Arquitectura de Software*, 2007. [2007]. Disponible en: http://www.microsoft.com/spanish/msdn/comunidad/mtj.net/voices/art110.asp

Reconocimiento Facial. 2007. [Disponible en: http://tecnociencia.es/monograficos/biometria/biometria4.html

REÍLLO, R. S. and Á. L. PUEBLA. *La Estandarización en el Campo de la Identificación Biométrica*, 2003. p.

RUIZ, A. P. *TÉCNICAS BIOMÉTRICAS PARA LA IDENTIFICACIÓN Y VERIFICACIÓN DE PERSONAS* 2007. [Disponible en: http://revista.robotiker.com/revista/articulo.do;jsessionid=7F436FE61C1FB3C69821FD9208A3ACFC?method=detalle&id=67

7 Anexos

Anexo 1.1 Comparación de características biométricas

	Ojos - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy Alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autent.	Ambas	Autent.
Interferencias	Gafas	Irritación	Suciedad, Heridas,	Artritis, reumatismo	Firmas fáciles o	Ruido, Resfriado

			asperezas,		cambiantes	
Utilización	Prisiones, servicios médicos, etcétera.	Prisiones, servicios médicos, etcétera.	Policía, industrial, prisiones	General	Industrial	Acceso remoto a bancos o bases de datos

Anexo 2.1 Estados de los Led del MSO 300

Estado	**Sensor**	**Led inferior**	**Led Superior**
Apagado	**Off**	**Off**	**Off**
Stand By	**Off**	**Parpadeo verde**	**-**
Estado mantenido o estado personalizado	**Off**	**Parpadeo Rojo**	**Parpadeo rojo**
Error en reconocimiento Usb	**Off**	**Rojo**	**Rojo**
Esperando por huella	**On**	**Off**	**-**
Esperando por huella alejada	**On**	**Verde**	**-**

Anexo 2.2 Características Técnicas de la canon 520

Resolución	4.00 M pixel
Resolución máxima	2272x1704
Resolución mínima	640x480

Tipo de sensor	CCD
Zoom óptico	Si
Zoom Digital	Si
Autofocus	Si
Enfoque manual	Si
Distancia de enfoque (cm)	47
Distancia de enfoque en macro (cm)	5
Tipo de almacenamiento	MultiMediaSecure Digital
Sensibilidad ISO	auto, 50, 100, 200, 400
Prioridad de apertura	Si
Prioridad de velocidad	Si
Velocidad mínima (sec)	15
Velocidad máxima (sec	1/2000
Disparo en ráfaga (fps)	1.9
Flash integrado	Si
Flash externo	Si
Medición de luz	Centre weightedEvaluativeSpot
Compensación de exposición	-2EV - +2EV with 1/3EV steps
Resolución máxima de vídeo	640x480
Visor óptico	Si
USB	USB 1.1
Formato de imagines	JPEG
Alimentación	2x AA
Peso bruto	180g.

Dimensiones (mm)	91x64x38

Anexo 2.1 Comparación entre distintos métodos de seguridad

Método de autentificación	Ventajas	Inconvenientes
Objeto físico (tarjeta, llave, pasaporte, etcétera.)	➢ Se puede reemplazar y proporcionar uno nuevo. ➢ Algunos métodos son bastante estándar, incluso al cambiar de país, instalación, etcétera.	➢ Puede ser robado. ➢ Puede usarse un objeto falso. ➢ Puede compartirse. ➢ Una persona puede registrarse con distintas identidades.
Clave conocida (password, PIN, etcétera.)	➢ Es simple y económico. ➢ Si existen problemas, puede ser reemplazado por una nueva, fácilmente.	➢ Puede ser crackeado o adivinado. ➢ Las buenas passwords son difíciles de recordar. ➢ Puede ser compartido. ➢ Una misma persona puede registrarse con distintas identidades.
Biométrico	➢ No puede ser perdido, robado, olvidado, adivinado, compartido, etcétera. ➢ Es relativamente sencillo comprobar si una persona tiene más de una identidad. ➢ Puede proporcionar un grado de seguridad superior a los otros métodos.	➢ Puede proporcionarse una característica falsa. ➢ No es reemplazable ni secreto. ➢ Si alguien se hace con una determinada característica biométrica de otra persona, no se podrá suministrar una nueva.

Anexo 3.1 Instalación de driver del MSO

En el directorio ...\MSO\mkit_3.10_protect\Launch.exe

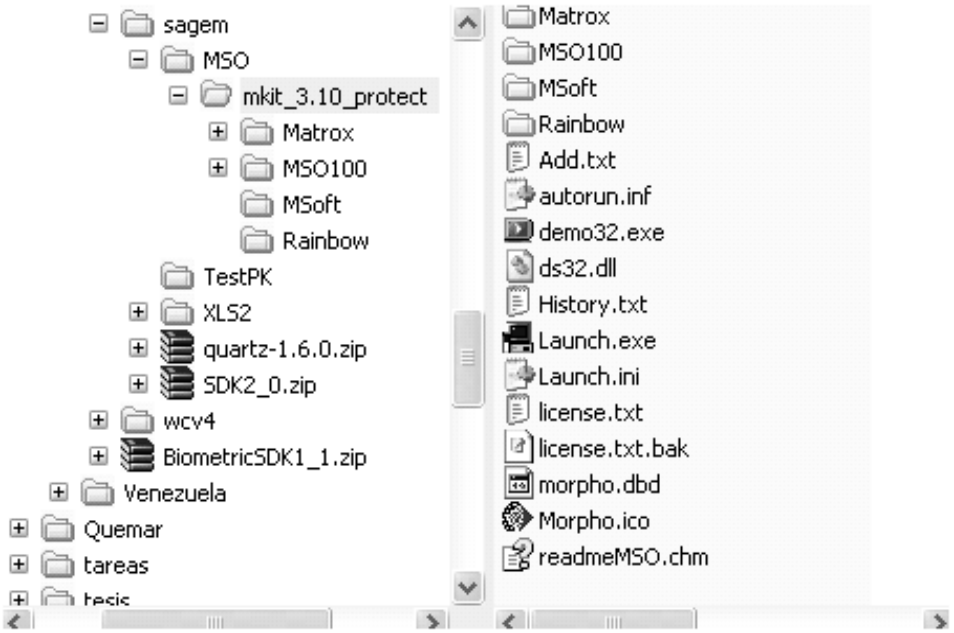

Figura 24 Instalador MSO 300

Al seleccionar el botón anterior muestra la ventana.

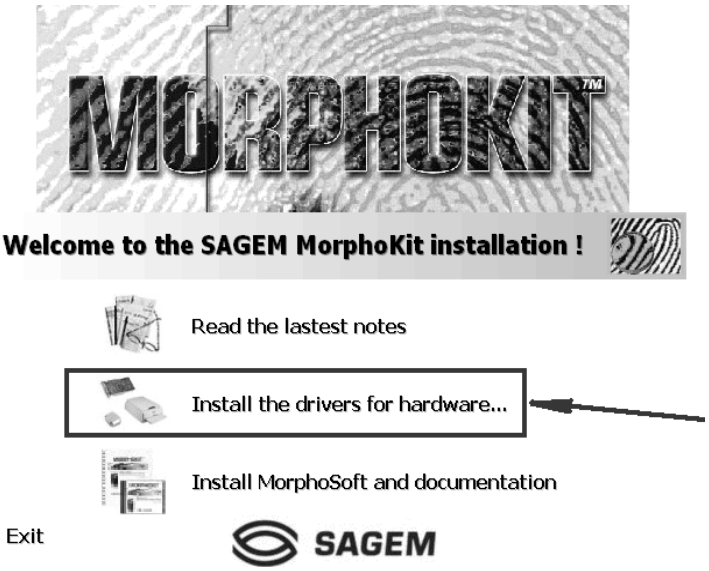

Figura 25

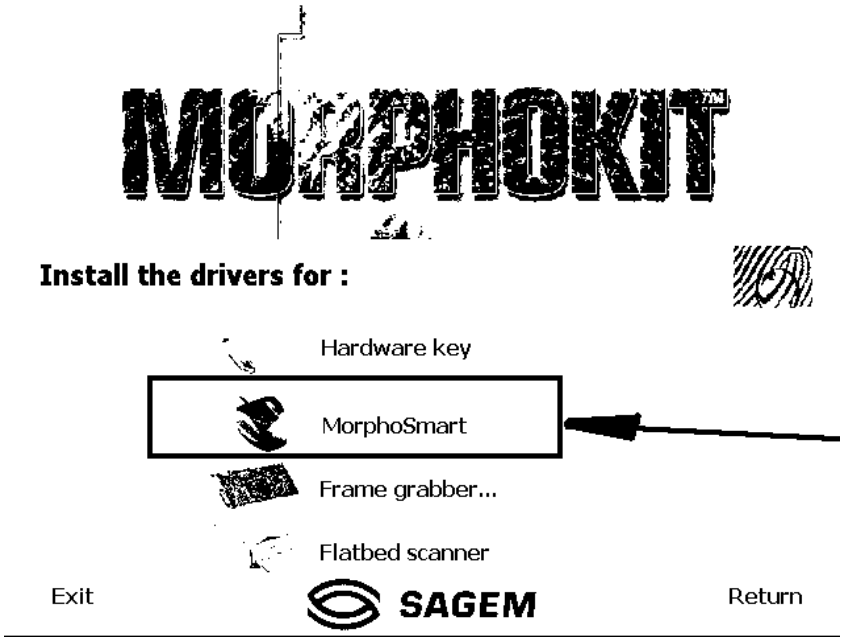

Figura 26

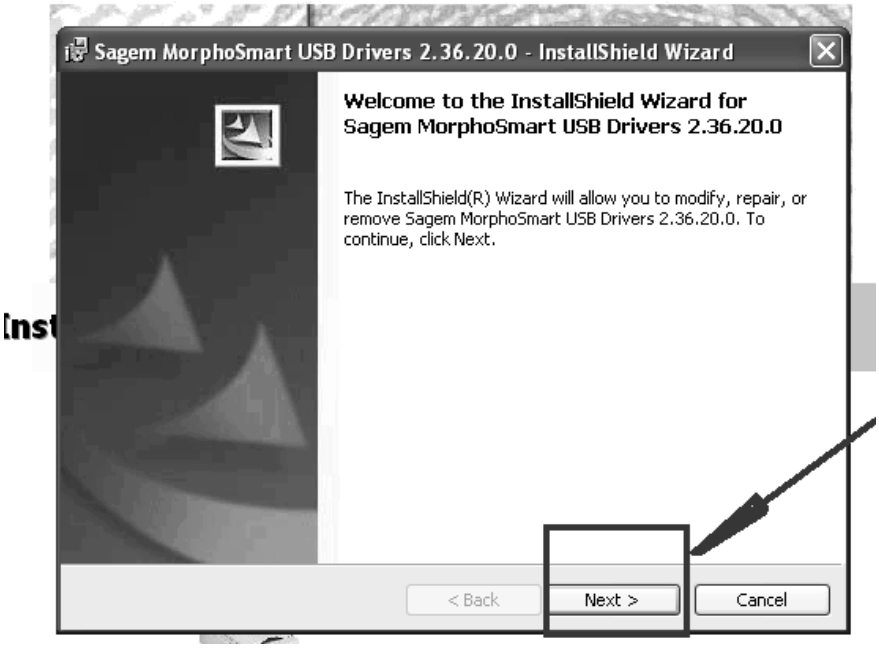

Figura 27

Para que el sistema este correctamente instalado se pruebe con el MSO 100, si los leds están parpadeando en verde esta correctamente, en caso que parpadeen en rojo es que aun el sistema no lo reconoce.

Anexo 3.2 Instalación del componente XLS2

Para realizar la instalación primeramente debemos chequear en el Administrador de Dispositivos que el driver señalado en la figura se encuentre instalado, en caso de no estarlo debemos buscarlo haciendo clic en la figura señalada en roja.

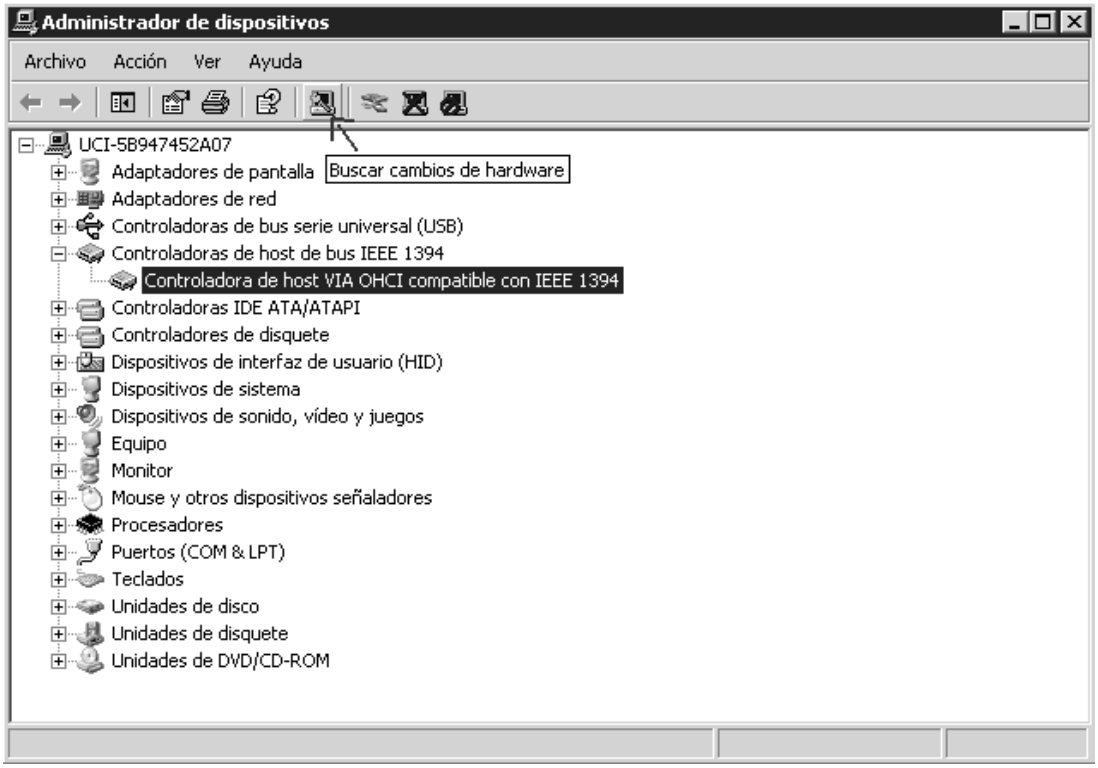

Figura 28

Primer paso

Ejecutamos desde nuestro CD de instalación el fichero tool_setup_XLS2.bat que se encuentra en la carpeta XLS2\CD_ROM_XLS2\ tool_setup_XLS2.bat

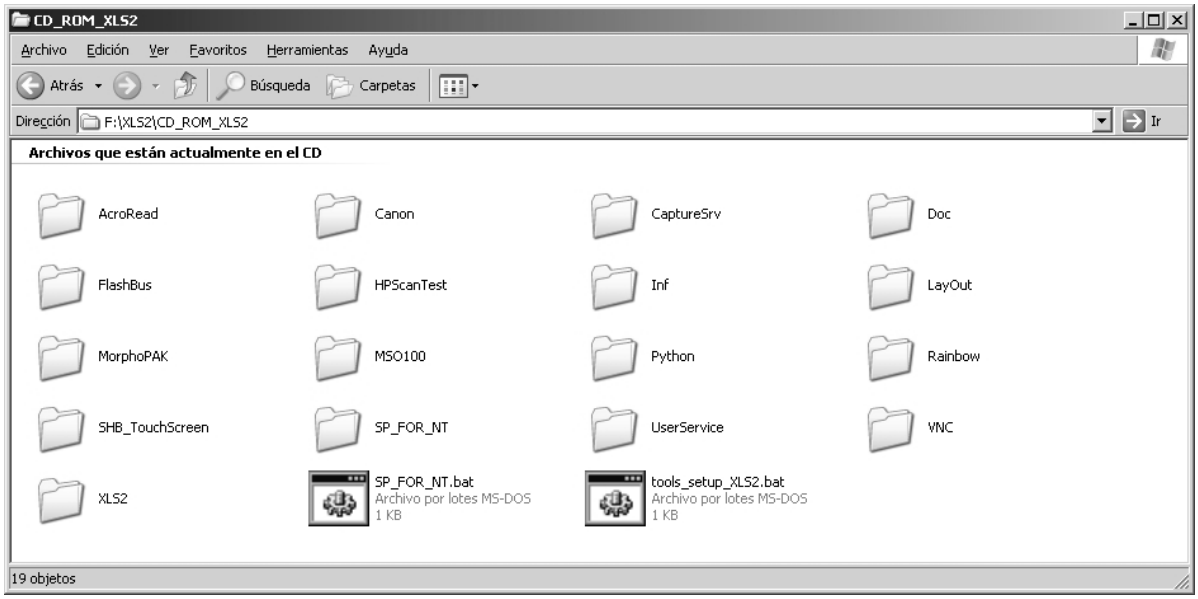

Figura 29

Segundo paso:

Abrimos la carpeta XLS2\CD_ROM_XLS2\CaptureSrv y ejecutamos el fichero setup.exe.

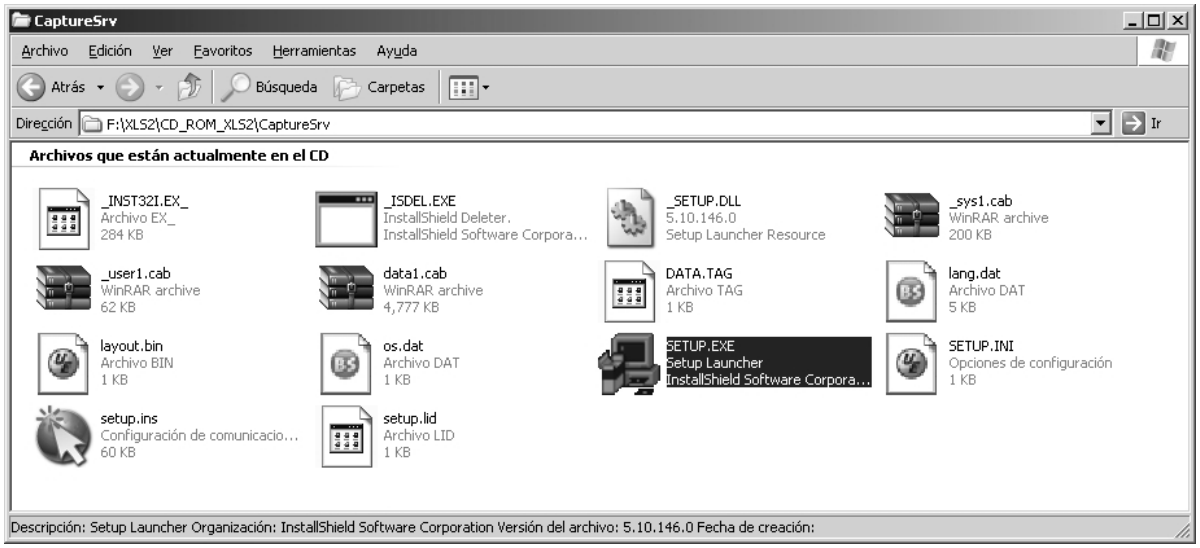

Figura 30

En la ejecución del mismo debemos seleccionar Capture DLL with IEEE card, al final pide reiniciar nuestra PC.

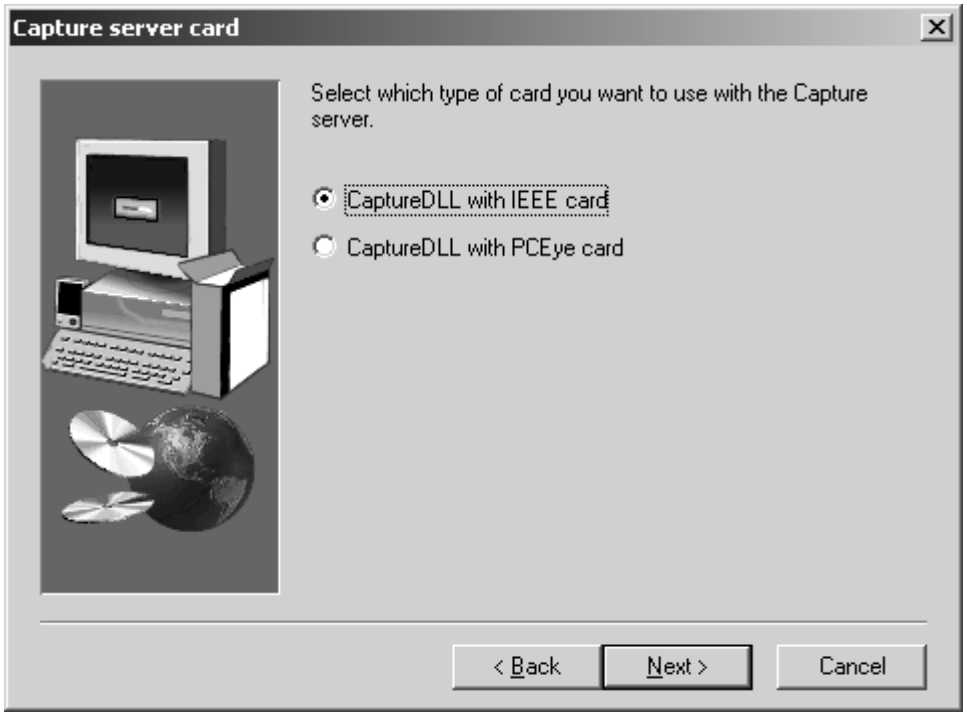

Figura 31

Tercer paso:

Después de haber reiniciado:

Ejecutamos el fichero setup.exe que se encuentra en la carpeta F:\XLS2\CD_ROM_XLS2\XLS2.

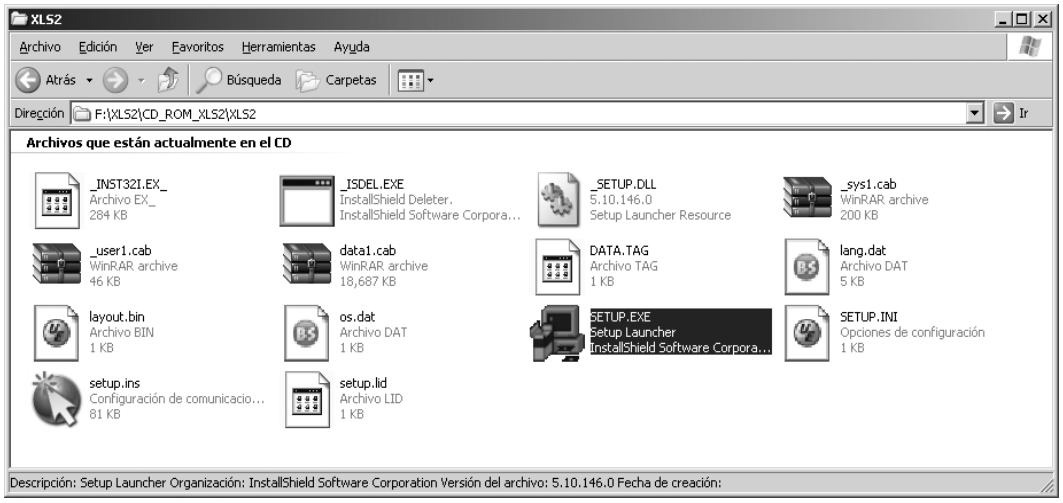

Figura 32

Al ejecutar el fichero nos sale la siguiente ventana con la ubicación de la carpeta

Booking que se creara en C:\ aquí damos clic en el botón Next.

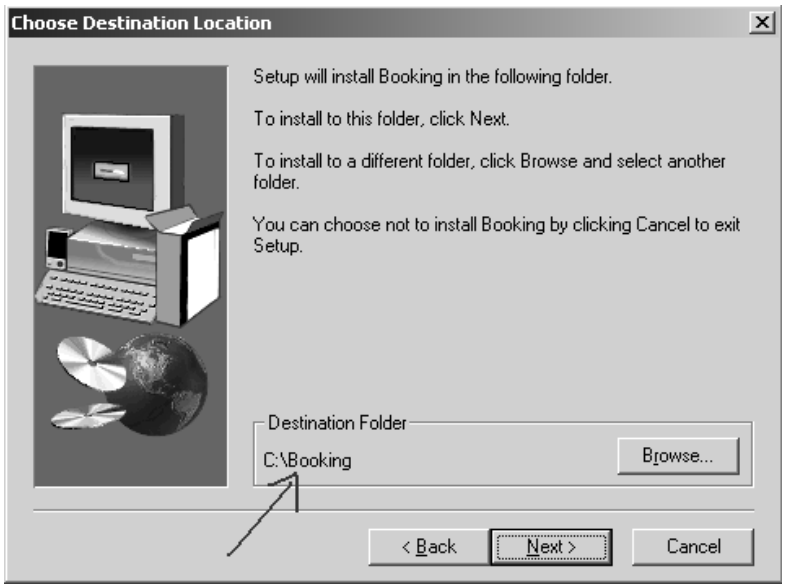

Figura 33

Importante para que no pase por alto este pasó. En la nueva ventana debemos dar clic en el botón Back para seleccionar los dispositivos con los que vamos a trabajar. La importante de este punto es que si se saltara, se perdería la configuración de los dispositivos que sería algo elemental para poder desarrollar una solución.

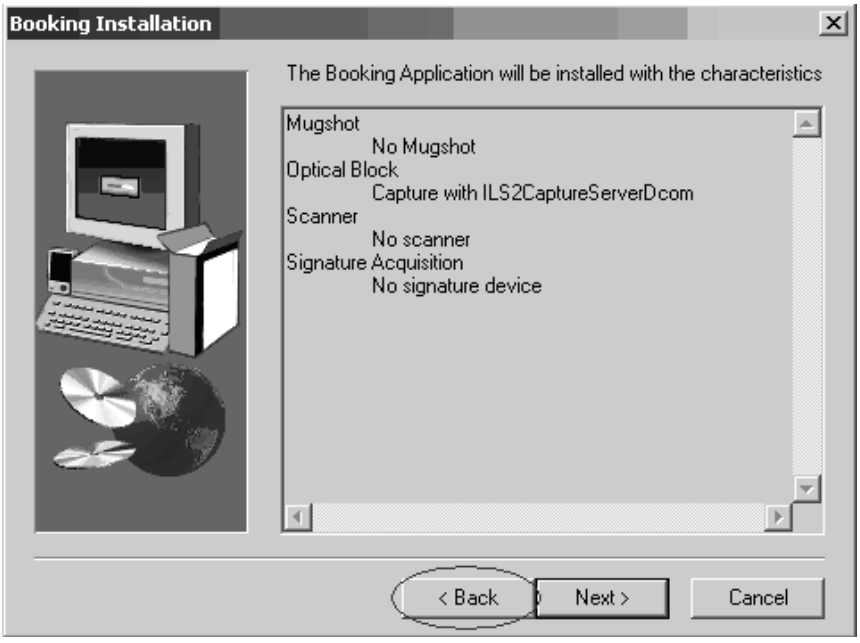

Figura 34

Seleccionamos la segunda opción y continuamos.

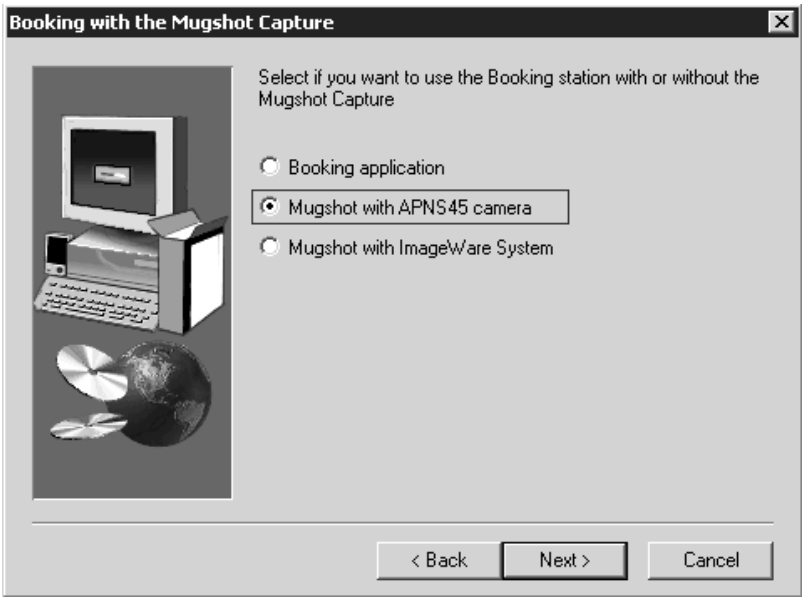

Figura 35

Seleccionamos la cuarta opción pues usaremos el MSO.

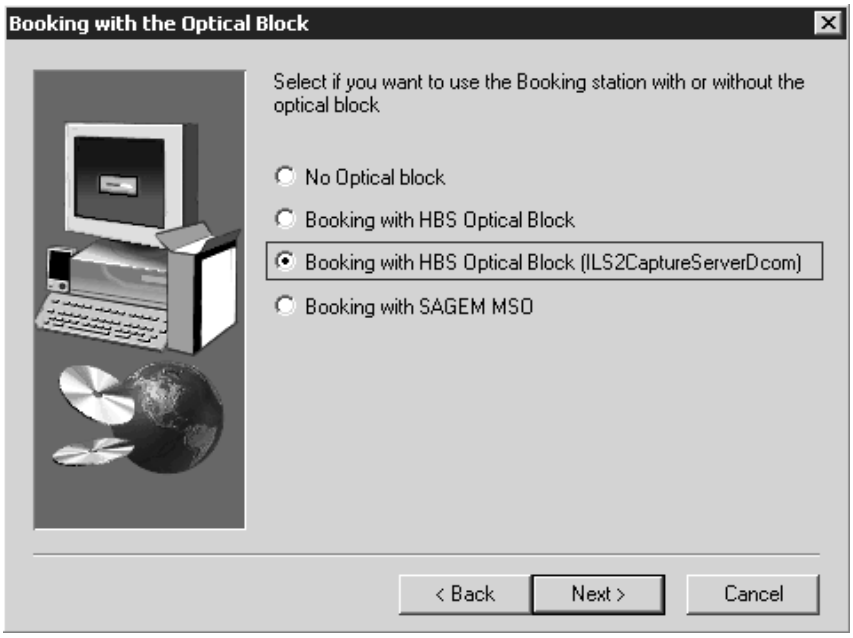

Figura 36

No tenemos en este momento un escáner por lo que seleccionamos la primera opción y continuamos.

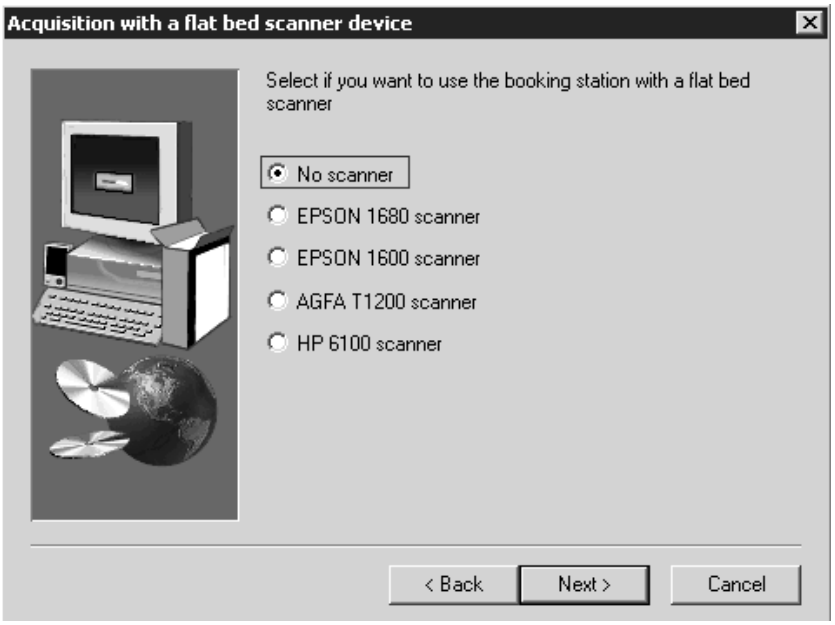

Figura 37

Seleccionamos la primera opción y continuamos

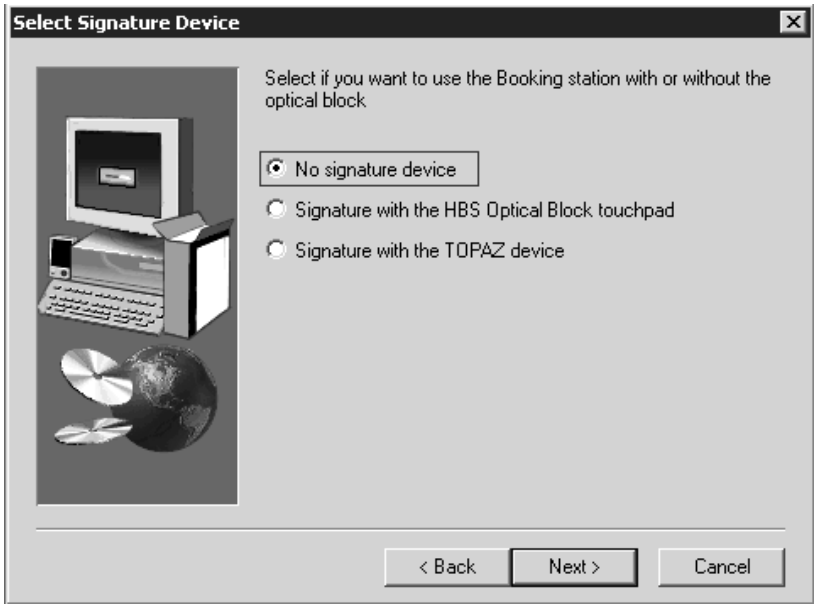

Figura 38

Continuamos

Figura 39

Se copia la licencia del dongle correspondiente en esta caso solo es utiliza el MorphoPACK,

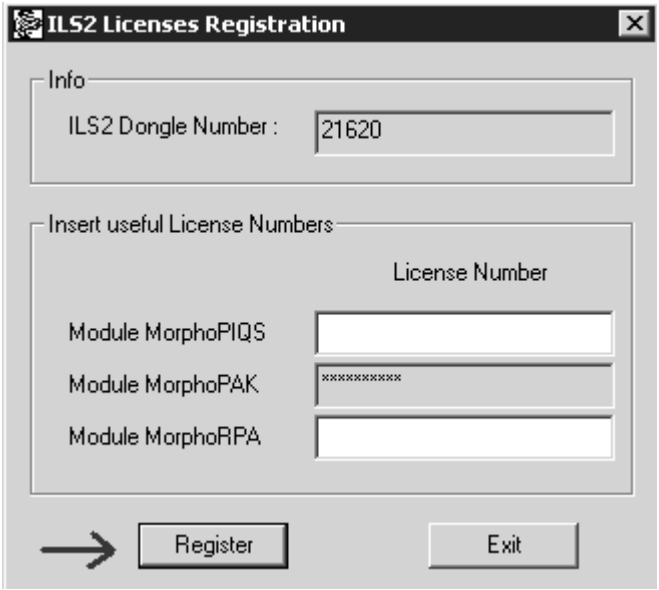

Figura 40

Esta ventana nos muestra que nuestra licencia es válida y aceptamos.

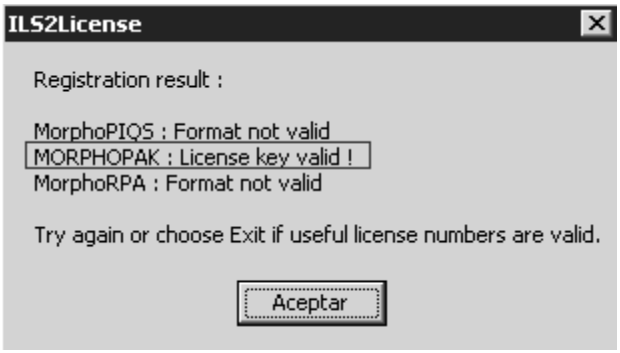

Figura 41

Cuarto paso:

Después de haber instalado el XLS2 nos dirigimos a carpeta C:\Booking\setup para registrar al mismo. Algunos de los errores que nos da Windows se deben a que algunas DLL no están debidamente registradas. Sobre todo esto suele suceder con los controles ActiveX.

El uso es:

Regsvr32 </u> </s> <nombre del fichero>

Por ejemplo:

regsvr32 **/s /c** XLS2.dll

Los parámetros opcionales </u> </s> significan lo siguiente:

</u> - lo utilizamos cuando queremos "desregistrar" una DLL.

</s> - modo "silencioso" - no despliega los mensajes durante la operación.

En la siguiente figura se muestran los ficheros a ejecutar.

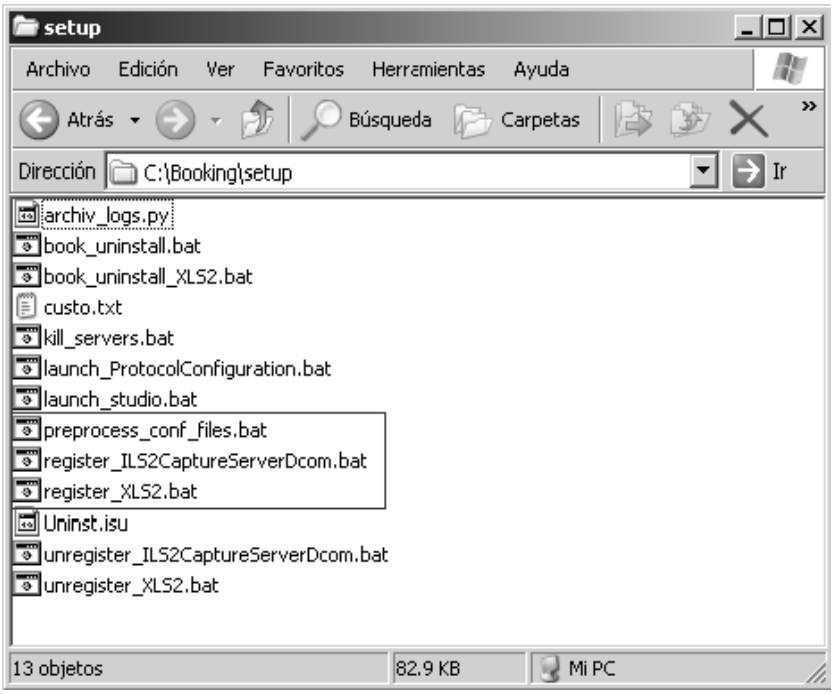

Figura 42

Quinto paso:

Después de haber ejecutado los *scripts* anteriores nos dirigimos a carpeta del CD F:\XLS2\Custo instalar los ficheros de personalización. Este paso es temporal, hasta que se cree el instalador final. Consiste en ejecutar un autoextraíble llamado sgm.exe que sobrescribe los ficheros necesarios en C:\Booking\sgm.

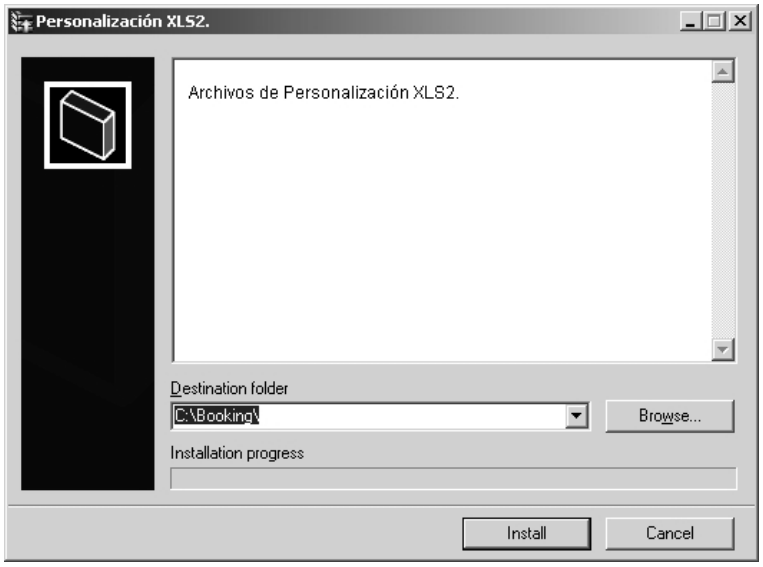

Figura 43

Cuando pregunte si desea sobrescribir todos los ficheros se le especificará: Yes to All

Después de terminar este paso el XLS2 está listo. Se puede utilizar la página web C:\Booking\exe\XLS2Wizard.htm para probar su funcionamiento correcto. Existirá un enlace directo en el escritorio a esa página Web. Se debe eliminar este enlace directo.