Prototipo funcional de biometría en dispositivos móviles, un acercamiento hacia el potencial de la biometría

David Felipe Toca Ávila

Universidad Piloto de Colombia
Sede Bogotá
Facultad de Ingeniería de Sistemas
Programa curricular de Ingeniería de Sistemas
Bogotá 2011

Prototipo funcional de biometría en dispositivos móviles, un acercamiento hacia el potencial de la biometría

David Felipe Toca Ávila
Código 0620407

Trabajo de Gradopresentado para optar al título de Ingeniero de sistemas

Asesor
Fredy Pérez Morales
Ingeniero de Sistemas

Universidad Piloto de Colombia
Sede Bogotá
Facultad de Ingeniería de Sistemas
Programa curricular de Ingeniería de Sistemas
Bogotá 2011

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C. Junio 16 de 2011

Dedicatoria

A mi hermana, que con su ejemplo, siempre me motiva a seguir adelante

A Dios quien siempre guía mis pasos

A mis padres, los cuales pusieron mucho esfuerzo para brindarme educación de calidad

Agradecimientos

A todos los profesores de la facultad de ingeniería, que participaron activamente en mi formación académica por mostrarme un mundo nuevo para mí, lleno de oportunidades y retos. A Fredy Pérez quien me brindo siempre su apoyo, y guio en el pro ceso de mi tesis. A Giovanni Fajardo, por sus enseñanzas dentro y fuera del salónde clase. A todos mis compañeros, por sus locuras que siempre lograban poner una sonrisa en mi rostro al final de cada jornada

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

pág

RESUMEN

Durante este documento se expondrá mi propuesta de un sistema que permita, por medio de tecnologías tendencia actual, realizar una identificación precisa de un sujeto dado. El caso de uso de esta aplicación es básicamente aportar a la seguridad de una empresa, un sistema de identificación de sus empleados, de tal modo que sea de fácil uso, más preciso que los sistemas convencionales, y basado en tecnologías convergentes y libres. El propósito de usar estas tecnologías se basa en el hecho que el proyecto propuesto no es otra cosa que un prototipo a futuro, por lo tanto, se deben implementar las tecnologías actualmente convergentes que más adelante serán usadas más ampliamente. Por otro lado se requieren que sean libres debido a que se busca crear una solución de bajo costo, adicionalmente, se pueden modificar para adaptarse a las necesidades que se lleguen a presentar.

Palabras Clave: Biometría, Seguridad, Móviles

INTRODUCCION

La biometría es una gran herramienta de seguridad, analiza patrones biológicos para identificar diferentes rasgos intrínsecos de una persona, en base a ciertas métricas definidas, un claro uso de este concepto es una cedula de ciudadanía, en donde se usa una huella y una foto (en conjunto con un numero) como identificador único. Su uso a través de los anos ha ido en aumento, hasta el punto que ahora es posible a través de computadores y otros dispositivos sensores (lector de huellas, cámaras, etc.) que procesan la información biológica, buscar ciertos patrones humanos únicos e intrínsecos de cada persona, con el propósito de autentificar su identidad.Lo que se pretende, es crear un prototipo funcional que permita poner al alcance de las pymes, a un bajo costo, un sistema de seguridad que haga uso de la biometría como método de identificación .Dicho desarrollo estará enfocado a dispositivos móviles, debido a que han probado ser una tecnología en auge, con múltiples beneficios, tales como multitarea, bajo costo en relación a otros dispositivos, etc.

1. GENERALIDADES

1.1 PLANTEAMIENTO DEL PROBLEMA

La seguridad es un elemento indispensable en toda empresa, para el caso de las pequeñas y medianas empresas es común el uso de mecanismos tales como tarjetas inteligentes, y servicio de celaduría, estos métodos sin embargo, no son 100\% seguros, tal y como lo asegura Antonio Ramos, Director de Consultoría y Auditoria de S21sec en su articulo[1]
"Los problemas que pueden aparecer con las técnicas de identificación tradicional, que con la biometría se evitan son por ejemplo, que las fotografías y las firmas van cambiando a lo largo del tiempo, los password y números secretos pueden ser robados, revelados u olvidados, los nombres y números de serie pueden ser modificados, y las tarjetas identificadoras pueden ser duplicadas o compartidas".
No obstante, este tipo de empresas no pueden adquirir sistemas de seguridad avanzados por sus altos costos. Es necesario entonces, diseñar y crear un mecanismo de bajo costo, que utilice un sistema de identificación que asegure un nivel de confiabilidad óptimo, dicho nivel puede ser conseguido teniendo en cuenta rasgos biométricos, citando nuevamente el artículo:

"Frente a esto, la biometría ofrece el mapeo digital intransferible y no decodificable por generar una clave de más de mil dígitos. La eliminación de fraudes por transgresión de identidad (eliminación de claves, códigos, tarjetas, etc.)...".

Además, debe estar a la par con las nuevas tecnologías convergentes, tales como la telefonía movil[2] (especialmente teléfonos con Android OS)[3] y sistemas orientados a servicios, dicho mecanismo debe ser de uso intuitivo.

1.2 JUSTIFICACION

Aunque la biométrica es un mecanismo de seguridad que permite tener un gran porcentaje de éxito, frente a otros métodos, el uso de este no es una opción explotada en pequeñas y medianas empresas, las cuales optan por otras alternativas, como el uso de tarjetas inteligentes para la autentificación de sus funcionarios, lo que deja un margen de error, que la biometríapodría solucionar. Esto se debe a la falta de iniciativas que permitan establecer un marco en el cual se puedan implementar soluciones biométricas a bajo costo, que las pymes puedan acceder. Es el propósito de este trabajo mostrar un prototipo que permita colocar la biometría dentro del alcance de este tipo de empresas.

1.3 ALCANCES

- El prototipo debe ser implementado para dispositivos móviles con sistema operativo android.
- El prototipo debe ser funcional
- Se debe emplear software libre
- No se contemplara el ingreso de la información a la base de datos documental por lo tanto, se asume que la información ya reside en dicha base de datos
- No se contemplara la creación de un administrador para la base de datos
- Debido a tiempo de desarrollo del que se dispone

1.4 LIMITES

- El tiempo de desarrollo de la solución debe ser no mayor a un ano
- El dispositivo debe poseer una cámara de mínimo 3 Megapixeles, y una capacidad de procesamiento no menor a 1Ghz
- El dispositivo móvil debe correr android 2.1
- Se hará uso del concepto de realidad aumentada, como un medio para visualizar información en el mundo real, e interactuar con ella

1.5 OBJETIVOS

1.5.1 Objetivo General. Desarrollar una aplicación móvil que pueda formar parte de una infraestructura de seguridad de bajo costo para una pequeña y mediana empresa, por medio del uso de software libre.

1.5.2 4. Objetivos Específicos

Implementar un sistema de base de datos, capaz de guardar y consultar información biométrica facial.

Implementar un algoritmo de reconocimiento facial, aplicable en un dispositivo móvil Android.

Aplicar en concepto de biometría por medio de la realidad aumentada, para detectar patrones humanos y permitir evidenciar visualmente esta autentificación.

Desarrollar un prototipo funcional, de una aplicación que permita, por medio de biométrica, el reconocimiento e identificación de personas por medio de sus rasgos faciales en un entorno controlado.

2. MARCO TEORICO

2.1 SEGURIDAD INFORMATICA

La Seguridad Informática suele ser la forma más habitual con la que nos referimos a todo aquello que tiene que ver con la seguridad de los ordenadores y los sistemas. Es un concepto muy conocido pero que está obsoleto. Hace hincapié en la seguridad de los sistemas, teniendo en cuenta las amenazasde carácter fundamentalmente tecnológico. La Seguridad Informática es un concepto de Seguridad que nació en la época en la que no existían lasredes de banda ancha, los teléfonosmóviles o los servicios de internet como las redes sociales o las tiendas virtuales. Es por ello que la Seguridad Informática suele hacer un especial énfasis en proteger los sistemas, es decir, los ordenadores, las redes y el resto de infraestructuras de nuestra organización. La Seguridad Informática es un concepto fundamentalmente técnico. El problema del enfoque de la Seguridad Informática es que suele perder de vista otros aspectos importantes para una organización y, en la mayoría de las ocasiones, cuando nos hablan de Seguridad Informática nos parece algo completamente alejado de nuestra actividad diaria.

Seguridad TIC (Seguridad de las Tecnologías de la Información y las Comunicaciones) Se trata de un enfoque más moderno, que incorpora el concepto de redes o infraestructura de comunicaciones. Hoy en día no concebimos el ordenador como un elemento aislado sino como unelemento conectado, y por otro lado, el ordenador ya no es el único elemento o dispositivo a proteger, sino que también hay que proteger las infraestructuras de comunicaciones, así como diversos dispositivos, como son los teléfonos móviles, PDA's, etc. La Seguridad TIC es un término mucho más amplio que la Seguridad Informática, pero sigue siendo de carácter fundamentalmente tecnológico.

2.1.1 Seguridad de la Información. Estamos ante el términomás amplio y conceptual de los tres. Se basa en que lo fundamental es proteger la información y en base a esta premisa se desarrollan todas los demás aspectos relativos a la seguridad y a las medidas que necesitamos aplicar, así como el lugar donde hay que aplicarla. Es un concepto que tiene en cuenta, no solamente la seguridad tecnológica, sino también otras facetas de la seguridad, como son, la seguridad desde el punto de vista jurídico, desde el punto de vista normativo y desde el punto de vista organizativo.

2.1.2 Objetivos Seguridad informática. La seguridad informática propone el cumplimiento de los siguientes objetivos.
La Integridad de la Información: es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La Disponibilidad u Operatividad de la Información: es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada, con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La Privacidad o Confidencialidad de la Información: es la necesidad de que la misma solo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitaran a esta última desarrollar un producto de características semejantes).

El Control sobre la información: permite asegurar que solo los usuarios autorizados pueden decidir cuándo y cómo permitir el acceso a la misma.

La Autenticidad: permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

Adicional mente pueden considerarse algunos otros aspectos, relacionados con los anteriores, pero
que incorporan algunas consideraciones particulares:

Protección a la Replica: mediante la cual se asegura que una transacción solo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.

No Repudio: mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.

2.2 BIOMETRIA

Es un término general utilizado para describir una forma alternativa característica o un proceso.

- Como una característica: Agente biológico medible (anatómicos y fisiológicos) y características de comportamiento que se puede utilizar para reconocimiento automático

- Como un proceso: Métodos automatizados de reconocimiento de una persona en base mensurables en la diversidad biológica (anatómica y fisiológica)

Los sistemas biométricos han sido investigados y probados para unos pocos décadas, pero solo recientemente han entrado en el publico la conciencia a causa de los altos usos de perfil, de uso en los medios de entretenimiento (aunque a menudo no realista) y un mayor uso por el público en a día las actividades del día. Como ejemplos de implementaciones podemos encontrar el Gobierno de los Estados Unidos, quienes incluyen el Automatizado de huellas dactilares del FBI por medio del Sistema de Identificación (IAFIS), el programa US-VISIT , el Transporte de Trabajadores Identificación de Verificación de Poderes (TWIC) del programa, y el registro Viajero (RT) del programa. Muchas compañíastambiénestán implementando tecnologíasbiométricas para asegurar aéreas, mantener registros de tiempo, y mejorar la comodidad del usuario. Por ejemplo, durante muchos años Disney Word ha empleado dispositivos biométricos para los dueños de bonos por temporada para simplificar el proceso del acceso a sus parques, garantizando al mismo tiempo que el tiquete es utilizado solo por la persona a la quien se le concedió. Un sistema biométricotípico se compone de cinco integrada componentes: un sensor se utiliza para recoger los datos y convertir la información a un formato digital. Algoritmos de procesamiento de señal realizar actividades de control de calidad y desarrollo de los datos biométricos plantilla. Un componente de base de datos mantiene la información que se compara con las plantillas. Un algoritmo de coincidencia que compara la plantilla biométrica nueva a unas o más plantillas mantenidas en la base de datos. Por último, un proceso de decisión (ya sea automatizados o humana asistida) utiliza los resultados de la comparación para hacer una decisión a nivel del sistema.
Las modalidades biométricascomúnmente aplicadas incluyen huellas dactilares, la cara, iris, voz, firma y la geometría de la mano. Muchos otras modalidades se encuentran en distintas fases de desarrollo y evaluación. No es una modalidad biométrica que sea mejor para todas las implementaciones. Hay muchos factores que deben tenerse en cuenta al implementar un dispositivo biométrico incluyendo la localización, riesgos de seguridad, tarea (identificación o verificación), que se espera número de usuarios, las circunstancias de usuario, los datos existentes, etc.También es importante tener en cuenta que las modalidades biométricas se encuentran en distintas etapas de la madurez. Reconocimiento de la huella Manual de comparación de las impresiones dactilares de reconocimiento ha estado en uso durante muchos años, y se ha convertido en un sistema automatizado de datos biométricosidentificacióntécnica en los últimas dos décadas. Las huellas dactilares tienen una superficie irregular de las crestas y los valles que forman un únicopatrón para cada individuo. Para la mayoría de las aplicaciones, el principal interés se centra en los patrones de canto en la articulación superior del dedo.

La precisión de un sistema biométrico se determina mediante una serie de las pruebas, comenzando con una evaluación del algoritmo de coincidencia precisión (evaluación de la tecnología), a continuación, evaluar el desempeño en un medio ambiente falso (evaluación de escenarios), seguido de pruebas en vivo en el lugar (evaluación operativa) antes de comenzar las operaciones completas. Cada evaluación tiene un propósito diferente e implica diferentes

tipos de análisis. Biométricostérminos, tales como el reconocimiento, verificacióneidentificación, se utilizan a veces al azar. Esto no es solo confuso, sino incorrecto, ya que cada término tiene un significado diferente. El reconocimiento es un términogenérico y no necesariamente implica tanto la verificación o identificación. Todos los datos biométricos sistemas de realizar el reconocimiento a personas que hayan sido registrados previamente, por otra parte, la verificación es una tarea en el sistema biométrico de confirmar la identidad de un individuo solicitado comparando una muestra tomada a una o más plantillas registradas previamente. La identificación es una tarea en el sistema biométrico intenta determinar la identidad de un individuo. Un biométrico se recoge y se compara con todas las plantillas en una base de datos. La identificación es cosed set cuando se sabe que la persona se sabe que existe en la base de datos, de otro modo es open set. Debido a estas variaciones, las diferentes estadísticas se deben utilizar para cada tarea. Verificación de la Tasa de falsa aceptación (FAR por sus siglas en ingles) el porcentaje de veces que un sistema produce una falsa aceptación, que se produce cuando una persona está mal adaptado a de otro individuo existente biométricos. Ejemplo: Frank dice ser John y el sistema verifica el reclamo.

2.2.1 Reconocimiento facial automatizado. El reconocimiento facial automatizado es relativamente un concepto nuevo. Desarrollado en los años 60, el primer sistema semiautomático para reconocimiento facial requería del administrador para localizar rasgos (como ojos, orejas, nariz y boca) en las fotografías antes de que este calculara distancias a puntos de referencia en común, los cuales eran comparados luego con datos de referencia.

En los años 70 Goldstein, Harmon, y Lesk, usaron 21 marcadores subjetivos específicos tales como el color del cabello y grosor de labios para automatizar el reconocimiento facial. El problema con estas soluciones previas era que se computaban manualmente. En 1988 Kirby y Sirobich aplicaron análisis de componentes principales, una técnicaestándar del algebra lineal, al problema del reconocimiento facial. Esto fue considerado algo así como un hito al mostrar que eran requeridos menos de 100 valores para cifrar acertadamente la imagen de una cara convenientemente alineada y normalizada.

En 1991 Tur y Portland utilizando las técnicas Eigenfaces, vieron que el error residual podía ser utilizado para detectar caras en las imágenes un descubrimiento que permitió sistemas automatizados de reconocimiento facial en tiempo real. Si bien la aproximación era un tanto forzada por factores ambientales, creo sin embargo un interés significativo en posteriores desarrollos de estos sistemas.

La tecnología inicialmente capturo la atención del público a partir de la reacción de los medios a una prueba de implementación en el SuperBowl de la NFL en enero de 2001, la cual capturo imágenes de vigilancia y las comparo con una base de datos de fotoarchivos digitales. Esta demostración inicio un muy requerido análisis sobre cómo usar la tecnología para satisfacer necesidades nacionales, mientras se tomaban en consideración las preocupaciones sociales

y de privacidad del público. Hoy la tecnología de reconocimiento facial está siendo utilizada para combatir el fraude de pasaportes, soporte al orden público, identificación de niños extraviados y minimizar el fraude en las identificaciones

2.2.2 Enfoques predominantes en Reconocimiento facial automatizado. Hay dos enfoques predominantes en el problema de reconocimiento facial:
El geométrico (basado en rasgos) y el fotométrico (basado en lo visual). Conforme a que el interés investigador en reconocimiento facial continúo, fueron desarrollados muchos algoritmos diferentes, tres de los cuales han sido bien estudiados en la literatura del reconocimiento facial:

- Análisis de componentes principales (Principal Component Analysis, PCA)
- Analisis lineal discriminante (Linear Discriminant Analysis, LDA)
- Correspondencia entre agrupaciones de grafos elásticos (Elastic Bunch Graph Matching, EBGM)

2.2.3 Análisis de componentes PRINCIPALES (Principal Component Analysis, PCA). PCA, comúnmente referida al uso de Eigenfaces, es la técnica impulsada por Kirby y Sirivich en 1988. Con PCA, el sondeo y la galería de imágenes deben ser del mismo tamaño y deben ser normalizadas previamente para alinear los ojos y bocas de los sujetos en las imágenes. La aproximación de PCA es luego utilizado para reducir la dimensión de los datos por medio de fundamentos de compresión de datos y revela la más efectiva estructura de baja dimensión de los patrones faciales.
Esta reducción en las dimensiones quita información que no es útil y descompone de manera precisa la estructura facial en componentes ortogonales (no correlativos) conocidos como Eigenfaces. Cada imagen facial puede ser representada como una suma ponderada (vector de rasgo) de los eigenfaces, las cuales son almacenadas en un conjunto 1D.
Una imagen de sondeo es comparada con una gallería de imágenes midiendo la distancia entre sus respectivos vectores de rasgos. La aproximación PCA típicamente requiere la cara completa de frente para ser presentada cada vez; de otra forma la imagen dará un resultado de bajo rendimiento.

2.2.4 Análisis lineal discriminante (Linear Discriminant Analysis, LDA). LDA es una aproximaciónestadística para clasificar muestras de clases desconocidas basadas en ejemplos de entrenamiento con clases conocidas. (Figura 1) Esta técnica tiene la intención de maximizar la varianza entre clases (ej. Entre usuarios) y minimizar la varianza de cada clase (Ej. De cada usuario). En la figura 1 donde cada bloque representa una clase, hay grandes variaciones entre clases, pero pequeñas en cada clase. Cuando se trata con datos faciales de alta dimensión, esta técnica enfrenta el problema de muestras de tamañopequeño que surge donde hay unnúmeropequeño de ejemplos de entrenamiento comparados a la dimensional dad del espacio de muestra.

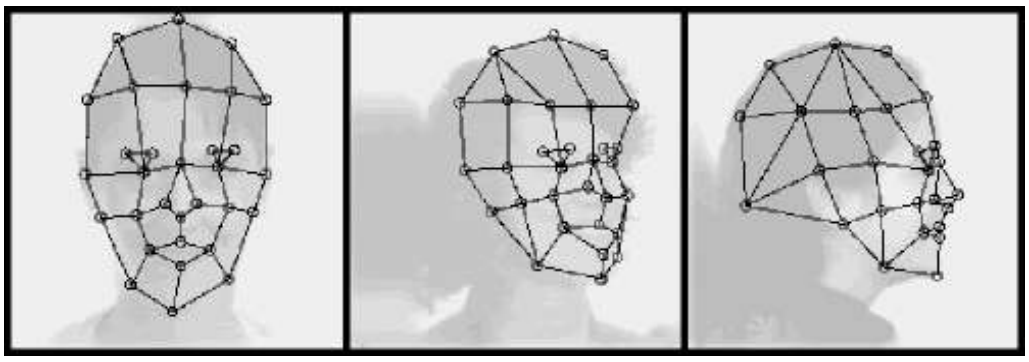
Figura 1 Ejemplo de seis clases usando LDA

2.2.5 Correspondencia entre agrupaciones de grafos elásticos (Elastic Bunch Graph Matching, EBGM). EBGM tiene en cuenta que las imágenes faciales reales tienen muchas características no lineales que no son tratadas en los métodos lineales de análisis discutidos previamente, tales como variaciones en la iluminación (Iluminación de exteriores vs. Interior fluorescente), postura (frontal vs. inclinada) y expresión (sonrisa vs. ceno fruncido).

Una ondeleta de transformación Gabor crea una arquitectura de enlace dinámico que proyecta el rostro sobre la planilla elástica. El Jet Gabor es un nodo en la planilla elástica, manifestado por círculos en la imagen debajo. El cual describe el comportamiento de la imagen alrededor de un pixel.

Este es el resultado de una convulsión de la imagen con un filtro Gabor, el cual es usado para detectar formas y extraer características utilizando procesamiento de imagen. (Una convulsión expresa la suma de solapamientos de las funciones en la mezcla de funciones entre sí) El reconocimiento está basado en la similitud de la respuesta del filtro Gabor a cada nodo Gabor.
Este métodobiológicamente basado utilizando filtros Gabor es un proceso ejecutado en la corteza visual de los mamíferosmás grandes. La dificultad con este método es el requerimiento de la precisa localización del punto de referencia el cual puede ser algunas veces logrado combinando los métodos PCA y LDA.

Figura 2 EjemploEBGM



A continuación se listan los métodos más conocidos para el reconocimiento facial.

Tabla 1 Métodos de reconocimiento facial

Métodos holísticos	**Métodos basados en características locales**	**Métodos híbridos**
• Análisis de componentes principales • Eigenfaces • Fisherface/Subspace LDA • SVM • ICA • LDA/FLA • PDBNN	• Métodos geométricos • Dynamic Link Architecture • Convolution Neural Networks	• Modular eigenfaces • Hybrid LF

2.2.6 Perspectiva de los estándares. La estandarización es una porción vital del avance del mercado y el estado del arte. Mucho trabajo se ha realizado en los estándares tanto nacionales (USA) como internacionales para facilitar la interoperabilidad y los formatos de intercambio de datos, lo que ayudara a facilitar el avance de la tecnología en una plataforma estandarizada. Las normas ANSI/INCITS (M1) 385-2004 e ISO 19794-5 de formato de intercambio de datos de reconocimiento facial son los mayores estándares en el área y están dirigidas al examen humano detallado de imágenes de rostros, verificación de identificación humana, e identificación y verificación facial automatizada. Estos estándares tienen en cuenta la interoperatibilidad entre los vendedores de reconocimiento facial.

Los estándares han establecido una imagen frontal definida y han irrumpido en sub-secciones dando tratamiento a imágenes frontales y no frontales (una imagen frontal es definida como una imagen a cinco grados del centro. Una imagen no frontal está definida por la ubicación de los ojos). Estos estándares dejan otras imágenes -tales como semiperfil- indefinidas, pero aseguran que las imágenes enroladas alcanzaran el estándar de calidad necesario tanto para reconocimiento automatizado de rostros como para inspección humana de imágenes de rostros. El trabajo está en proceso en los niveles nacionales e internacionales para actualizar los estándares de datos de rostro 3D. ANSI

NIST ITL 1-2000 está siendo también actualizada para incluir más y mejor información para imágenes faciales del tipo 10. Hay también trabajo relacionado con el nivel internacional, para proveer de una guía a los fotógrafos sobre como capturar mejor las imágenes faciales para reconocimiento automatizado. Estos estándarestambién facilitan el uso de información de rostros en aplicaciones que tienen capacidad de almacenamiento limitada (Ej. Pasaportes, visas, licencias de conducir). Otros estándares como INCITS 398-2005 (Common Biometric Exchange Formats Framework, CBEFF), o Marco de trabajo de Formatos para Intercambios Comunes de Biometría, tratan específicamente con los elementos utilizados para describir los datos de biometría de forma común.

La especificación INTCITS 358-2002 BioAPI (ApplicationProgramming Interface) define la interface de programación de la aplicación y la interface del proveedor del servicio para una interface de tecnologíabiométricaestándar.

Las organizaciones estándar nacionales e internacionales continúan trabajando en la progresión de los estándares en un sentido que facilite el crecimiento, el avance y la interoperabilidad.

2.3 HIPÓTESIS

¿Será posible construir una aplicación de seguridad prototipo que usen la biometría como sistema de identificación, que sea rentable para una pyme, y además operada a través de dispositivos móviles?

3. DISEÑO METODOLOGICO DE LA INVESTIGACION

Para lograr los objetivos propuestos, es necesario diseñar y construir un software que permita validar la hipótesis anteriormente mencionada, para ello se va a hacer uso de una metodología de construcción de software conocida como desarrollo basado en iteraciones.

Se selecciono esta metodología, debido a que permite minimizar los procesos que tardan tiempo, para entregar avances o compilados por módulos, documentando todo el proceso y facilitando de transferencia de conocimientos. El ciclo de desarrollo será el siguiente:

- Inicio
- Requerimientos
- Análisis y Diseño Global
  - Estructuración
  - Diagramas
  - Diseño
- Iteración de Análisis por Etapas
  - Diagramas por Etapa
  - Términos y condiciones de entrega
- Iteración de Desarrollo por Etapas
  - Desarrollo de Etapa
  - Entrega de Etapa
- Validación del producto integro
- Cierre

3.1 INICIO

En esta etapa se revisa brevemente la finalidad del producto, así como sus objetivos propuestos, y se realiza un levantamiento de información.

3.2 REQUERIMIENTOS

En esta etapa se realiza la búsqueda y obtención de los requerimientos generales, dichos requerimientos surgen las necesidades que el programa plantea satisfacer, y nos proveen una base para la planificación del contenido

técnico de las iteraciones, estimación de costos, y tiempo de desarrollo de la aplicación.
Al finalizar esta etapa se espera que el desarrollador posea un mejor entendimiento acerca del producto respecto a las necesidades del cliente.

3.3 ANALISIS Y DISEÑO GLOBAL.

En esta actividad se especifican los requerimientos y se describen sobre cómo se van a implementar en los sistemas

Estructuración. Analizando los requisitos a una especificación, se desarrollar una arquitectura para el sistema que satisfaga las necesidades previamente detectadas, y los recursos tecnológicos a utilizar.

Diagramas. En esta fase se transformar los requisitos al diseño del sistema, definiendo diagramas de caso de uso y secuencia del sistema en general.

Diseño. El objetivo final de este flujo de trabajo es producir un modelo conceptual y genérico como abstracción del sistema, de modo que sea posible visualizar globalmente dicha solución. También se supone un punto de partida para implementación capturando requisitos de las clases de análisis.

3.4 ITERACION DE ANALISIS POR ETAPAS

Esta etapa involucra el rediseño e implementación de una tarea de la lista de control de proyecto, y el análisis de la versión más reciente del sistema. La meta del diseño e implementación de cualquier iteración es ser simple, directa y modular, para poder soportar el rediseño de la etapa o como una tarea añadida a la lista de control de proyecto. El código puede, en ciertos casos, representar la mayor fuente de documentación del sistema. El análisis de una iteración se basa en la retroalimentación del usuario y en el análisis de las funcionalidades disponibles del programa. Involucra el análisis de la estructura, modularidad, usabilidad, confiabilidad, eficiencia y eficacia (alcanzar las metas).

3.5 VALIDACIÓN DEL PRODUCTO INTEGRO

En esta fase se realizan pruebas de sistema, corroborando que los casos de uso definidos previamente para el sistema se cumplan.

4. DESARROLLO METODOLOGICO DE LA INVESTIGACION

4.1 INICIO

La finalidad del producto es crear un prototipo de bajo costo que permita realizar una identificaciónbiométrica por medio del uso de dispositivos móviles. Los objetivos para este proyecto están especificados en la sección 6 de este documento.

4.2 REQUERIMIENTOS

Se realizo una revisión de las funcionalidades básicas de un sistema de reconocimiento, en base a esto se identificación las siguientes funcionalidades:

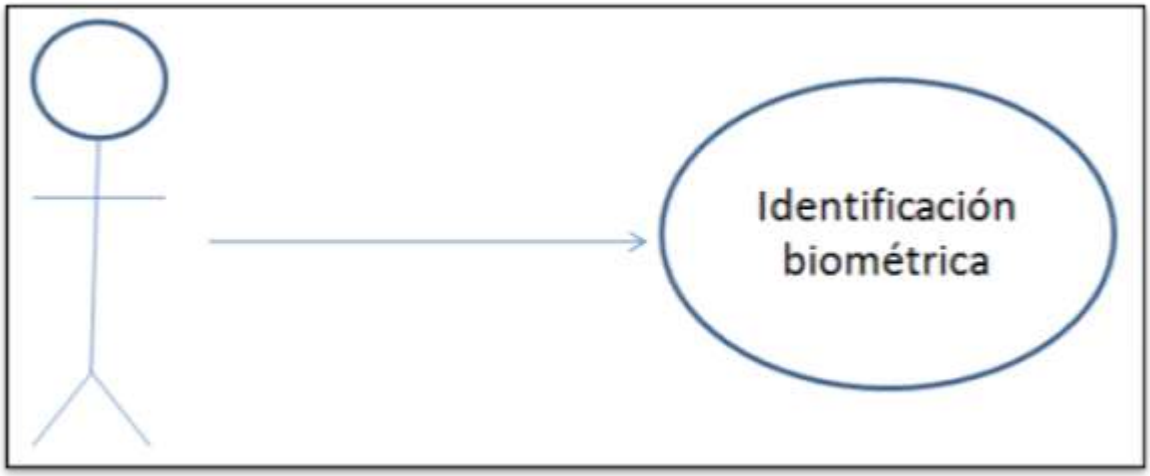
- Log de la hora de ingreso y partida
- Identificación de la persona
- Permisos de ingreso (ej. ingreso de equipos)
- Ingreso de invitado

4.3 ANALISIS Y DISEÑO GLOBAL.

4.3.1 Estructuración. Analizando los requisitos a una especificación, se idea un sistema que satisfaga las necesidades previamente detectadas, en esta fase se define la arquitectura y los recursos tecnológicos a utilizar.
Se analizaron los requerimientos, y en base a esto, se definió una arquitectura de cliente servidor, de este modo es posible que el sistema tenga otros clientes alternativos a la aplicaciónmóvil, además es necesario un servidor en donde fuese posible guardar gran cantidad de informaciónbiométrica. Adicionalmente, el uso de webservice entre el cliente y el servidor, facilita la comunicación entre ambos, y hace al sistema más sostenible.

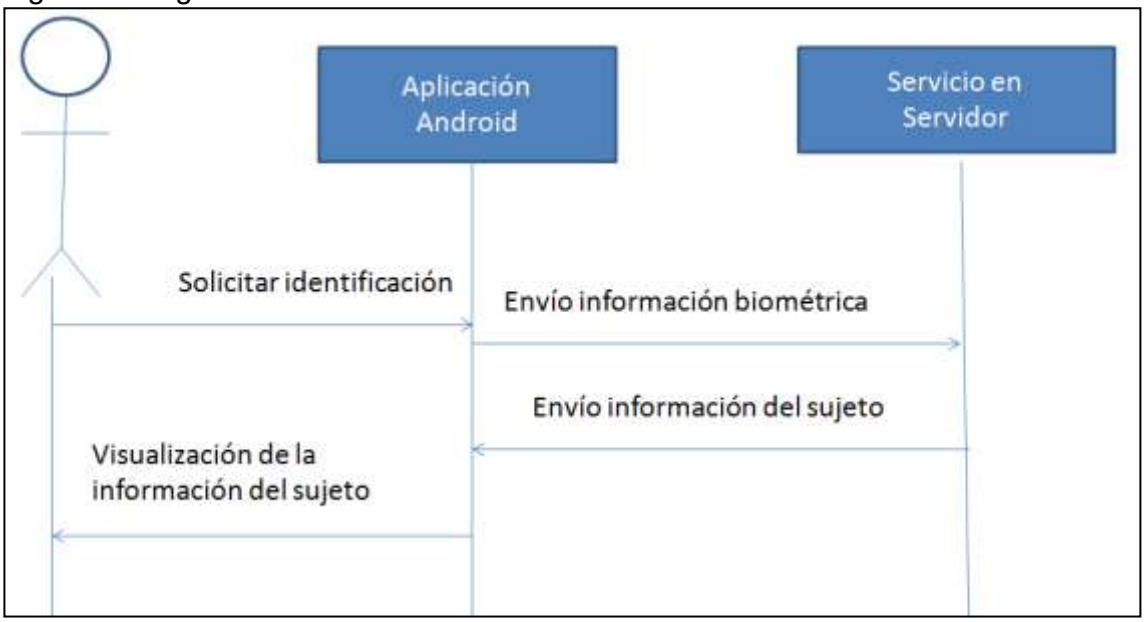
4.3.2 Diagrama de caso de uso. Se presenta el diagrama de casos de uso para la identificación biométrica.

Figura 3 Diagrama de caso de uso



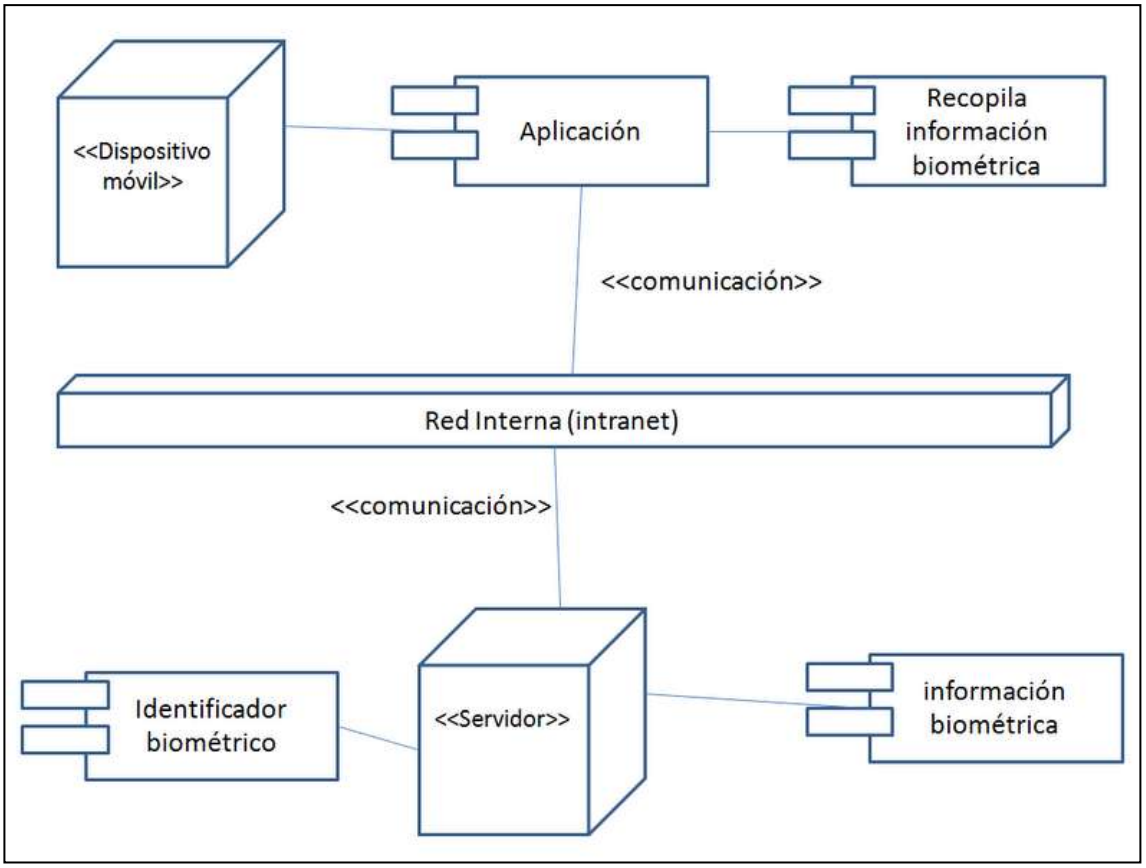
4.3.3 Diagrama de secuencia. Se presenta el diagrama de secuencia de uso para la identificación biométrica.

Figura 4 Diagrama de secuencia



4.3.4 Diseño. El diseño del sistema general, está conformado por la aplicaciónmóvil y sus componentes, el web servicie por medio del cual se comunicara con el servidor, que poseerá un servicio en el cual usara la informaciónbiométrica para retornar la informaciónde la persona identificada, dicho diseño se puede observar a continuación.

Figura 5 Diagrama general



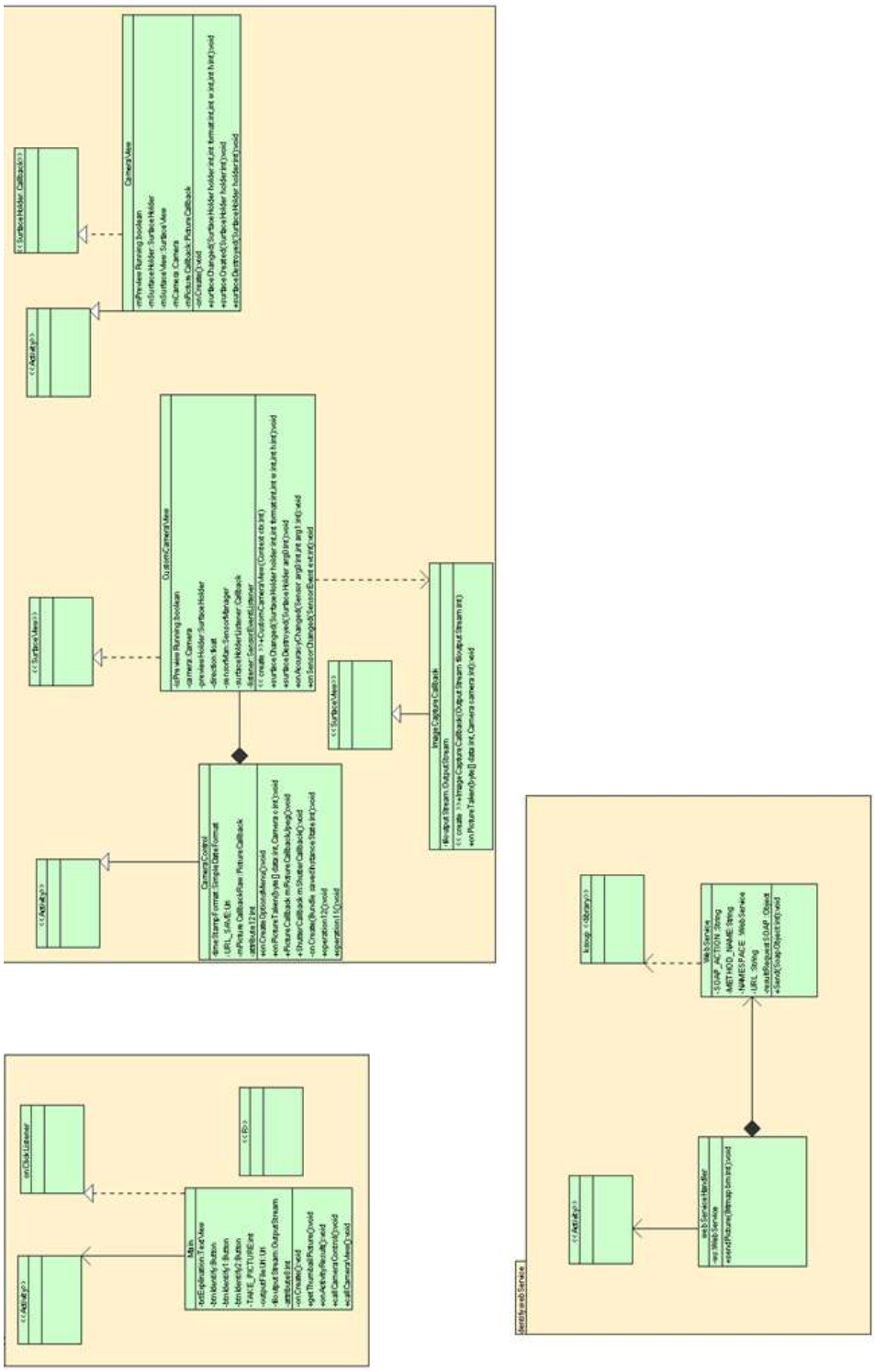
4.4 ITERACION DE ANÁLISIS POR ETAPAS

Tomando en cuenta las tecnologías a aplicar, y las relaciones entre los componentes del sistema, se identificaron las siguientes etapas.

4.4.1 Etapa uno - Cliente android. En esta etapa se construirá la aplicación para el dispositivo móvil, se supone la base para la aplicación cliente.

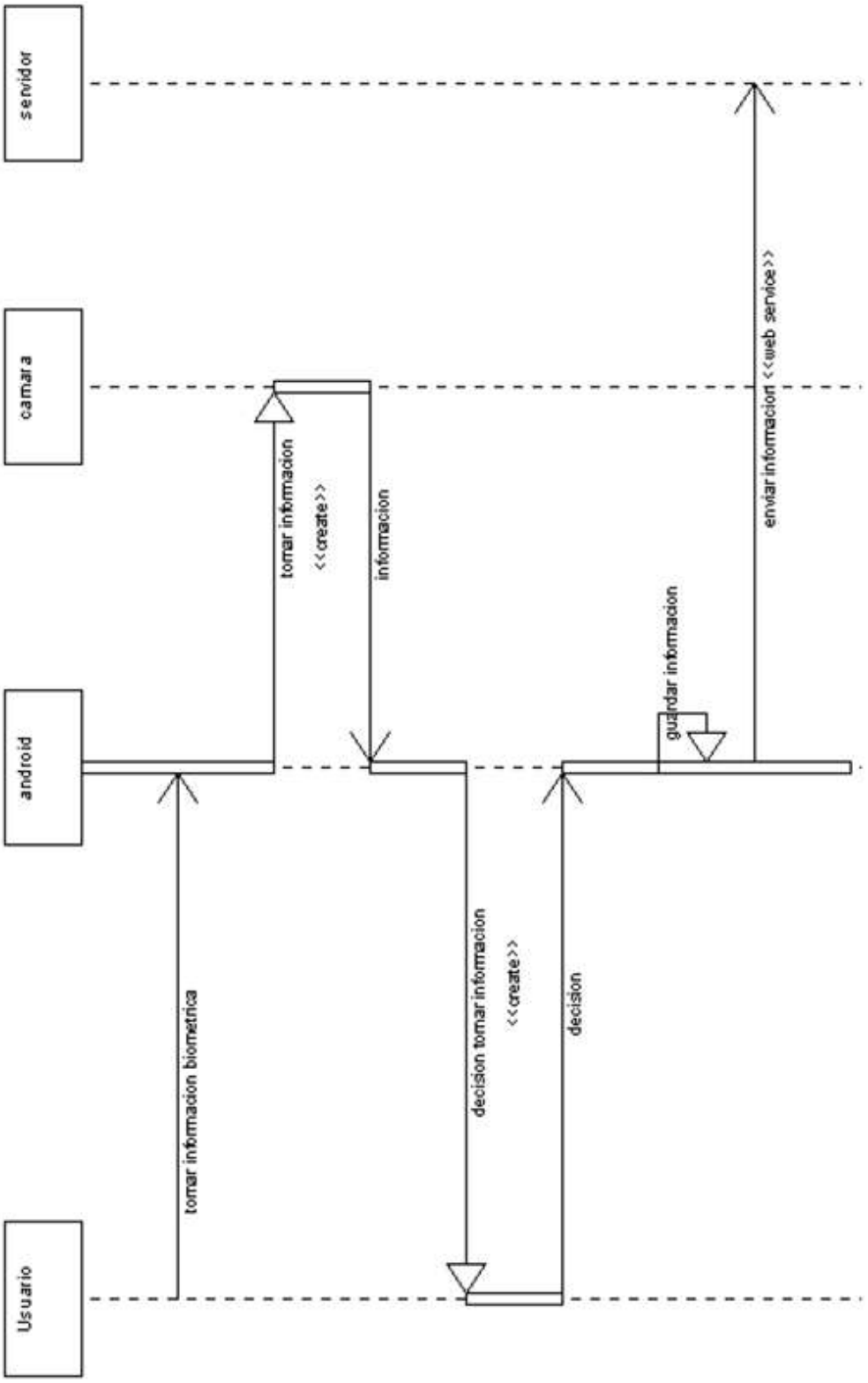
4.4.1.1 Diagrama de clases. Se presenta el diagrama de clases para la identificación biométrica.

Figura 6 Diagrama de clases etapa 1



4.4.1.2 Diagrama de secuencia

Figura 7 Diagrama de secuencia etapa 1



4.4.1.3 Requerimientos

Tabla 2 R-001 Ajustar orientación cámara

Descripción	Muestra al usuario la cámara dependiendo de la orientación del dispositivo (landscape/ portrait)
Tipo	Interfaces
Entrada	Orientación del dispositivo
Resultado	cámara se a justa a la orientación del dispositivo

Tabla 3 R-002 Activar la cámara

Descripción	Activa la cámara del dispositivo cuando el usuario selecciona identificar usuario
Tipo	Recursos, Ambiente físico
Entrada	Petición del usuario para activar la cámara
Resultado	El sistema controla la cámara

Tabla 4 R-003 Procesar imagen tomada

Descripción	Después de tomar la foto, el usuario debe decidir si descarta o guarda dicha foto, para su identificación
Tipo	Recursos, Ambiente fisico
Entrada	Imagen tomada decisión del usuario (bytes). Apuntador a la cámara. Directorio de destino. Decisión del usuario.
Resultado	En caso que el usuario seleccione Guardar, el sistema transforma la información imagen de tipo bitmap y la guarda en el directorio de destino En caso contrario, el programa regresara al menú de inicio

Tabla 5 R-004 Usar herramientas nativas

Descripción	El sistema deberá usar las herramientas nativas del sistema en la medida que sea posible, para mejorar la experiencia del usuario
Tipo	Recursos, Ambiente físico
Entrada	Petición del usuario para activar la cámara. Apuntador a la cámara.
Resultado	Si se poseen dichas herramientas, quedan a la disposición del usuario.

Tabla 6 R-005 Enviar información a servidor

Descripción	Enviar información biométrica al servidor
Tipo	Imagen a enviar Url del servicio. Namespace del servicio. Método de servicio. Archivo descriptor del servicio (wsdl)
Entrada	Petición del usuario para activar la cámara
Resultado	Se envió la información al servidor y se visualiza el mensaje identificando. En el caso que no se tenga conexión al servidor, el sistema deberá alertarlo y volver al menú de inicio.

Tabla 7 R-006 Visualizar información de forma grafica

Descripción	Posterior al envió de la información, el sistema deberá activar nuevamente la cámara (sin las herramientas del dispositivo), de modo que al obtener la información de la persona, pueda visualizarla por medio de RA.
Tipo	Recursos, Ambiente físico
Entrada	Notificación del envió de la información exitoso
Resultado	Se activo correctamente la información de la cámara sin las herramientas del dispositivo.

Tabla 8 Caso de uso-001

Descripción	Permite al usuario visualizar correctamente la cámara en cualquier posición
Actores	Usuario del sistema
Precondiciones	Ninguna
Flujo norma	El actor cambia la orientación del dispositivo La cámara cambia de disposición para ajustarse landscape/ portrait
Flujo alternativo	n/a
Pos-condiciones	Se debe visualizar un cambio de posición

Tabla 9 Caso de uso-002

Descripción	Permite al sistema controlar la cámara
Actores	
Precondiciones	Ninguna
Flujo norma	El actor pulsa sobre el botón de identificación El sistema decide qué tipo de imagen se va a guardar

	raw/.jpg El sistema abre un canal de salida OutputStream El sistema define la superficie y su vista
Flujo alternativo	El sistema modifica las propiedades de la ventana actual, de modo que se visualiza en modo completo, sin título, y con las notificaciones desactivadas Si se descarta la foto, la aplicación también descarta la información y vuelve al menú principal.
Pos-condiciones	Se debe continuar con el envió de la información al servidor

Tabla 10 Caso de uso-003

Descripción	Permite al sistema controlar el llamado callback de la cámara
Actores	Usuario del sistema
Precondiciones	Ninguna
Flujo norma	El actor toma la foto El actor decide si dicha foto debe ser elegida o descartada. En caso de ser elegida, el sistema debe inicializar una clase de tipo PictureCallback que almacene la información en bytes Dicha información debe luego ser convertida a un bitmap, y posteriormente la envía para a su vez ser enviada al web service
Flujo alternativo	Si se descarta la foto, la aplicación también descarta la información y vuelve al menú principal.
Pos-condiciones	Se debe continuar con el envió de la información al servidor

Tabla 11 Caso de uso-004

Descripción	Permite al sistema usar las funciones nativas de la cámara.
Actores	Usuario del sistema
Precondiciones	Ninguna
Flujo norma	El actor pulsa sobre el botón de identificación El sistema activa la cámara. El sistema debe enviar un intent con el objetivo de buscar herramientas nativas que pueda usar la cámara ej. Foco. En caso de que encuentre dichas herramientas se deben poner a disposición del usuario.
Flujo alternativo	En caso que el dispositivo no posea las herramientas de la versión 2.1, el sistema usara una cámara sin herramientas.
Pos-condiciones	Se debe activar la cámara.

Tabla 12 Caso de uso-005

Descripción	Permite al usuario enviar la información al servidor para su autentificación.
Actores	Usuario del sistema
Precondiciones	Información biométrica del sujeto tomada
Flujo norma	El sistema tomara la información biométrica y la enviara al servidor
Flujo alternativo	Si no se posee conexión al servidor, la aplicación informara esto al usuario, y regresara al menú de inicio
Pos-condiciones	Se envía la información por medio de un web servicie al servidor

Tabla 13 Caso de uso-006

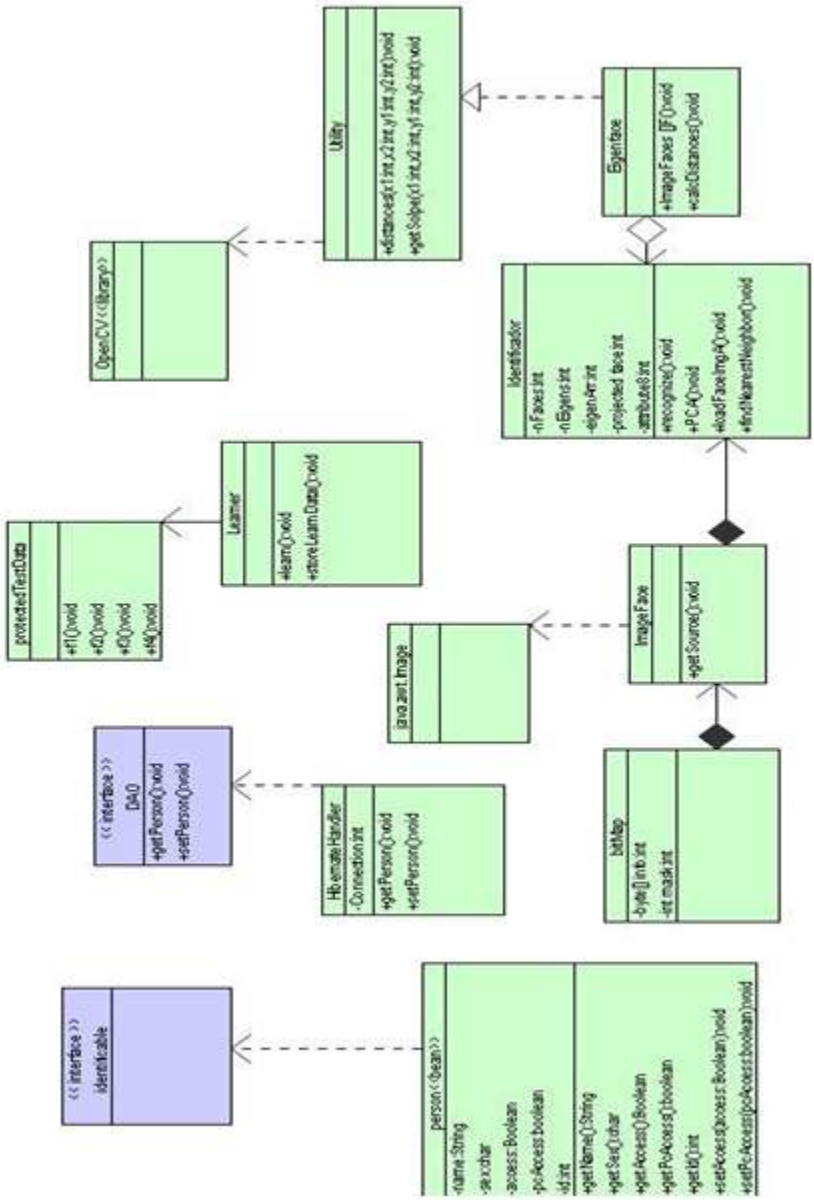
Descripción	Permite al sistema visualizar la cámara, para posteriormente mostrar la información con RA.
Actores	Usuario del sistema
Precondiciones	Información biométrica del sujeto tomada
Flujo norma	Una vez la foto es tomada y enviada al servidor, el sistema debe activar nuevamente la cámara, esta vez en espera de la información biométrica
Flujo alternativo	Si dicha información no llega en un tiempo prudente (timeout), el sistema informara que no es posible acceder al servidor
Pos-condiciones	Envió de información biométrica al servidor.

4.4.2 Etapa dos - biometría en Servidor

En esta etapa se construirá la lógica de la identificaciónbiométrica en el servidor, capaz de procesar personas a travésde biometría facial.

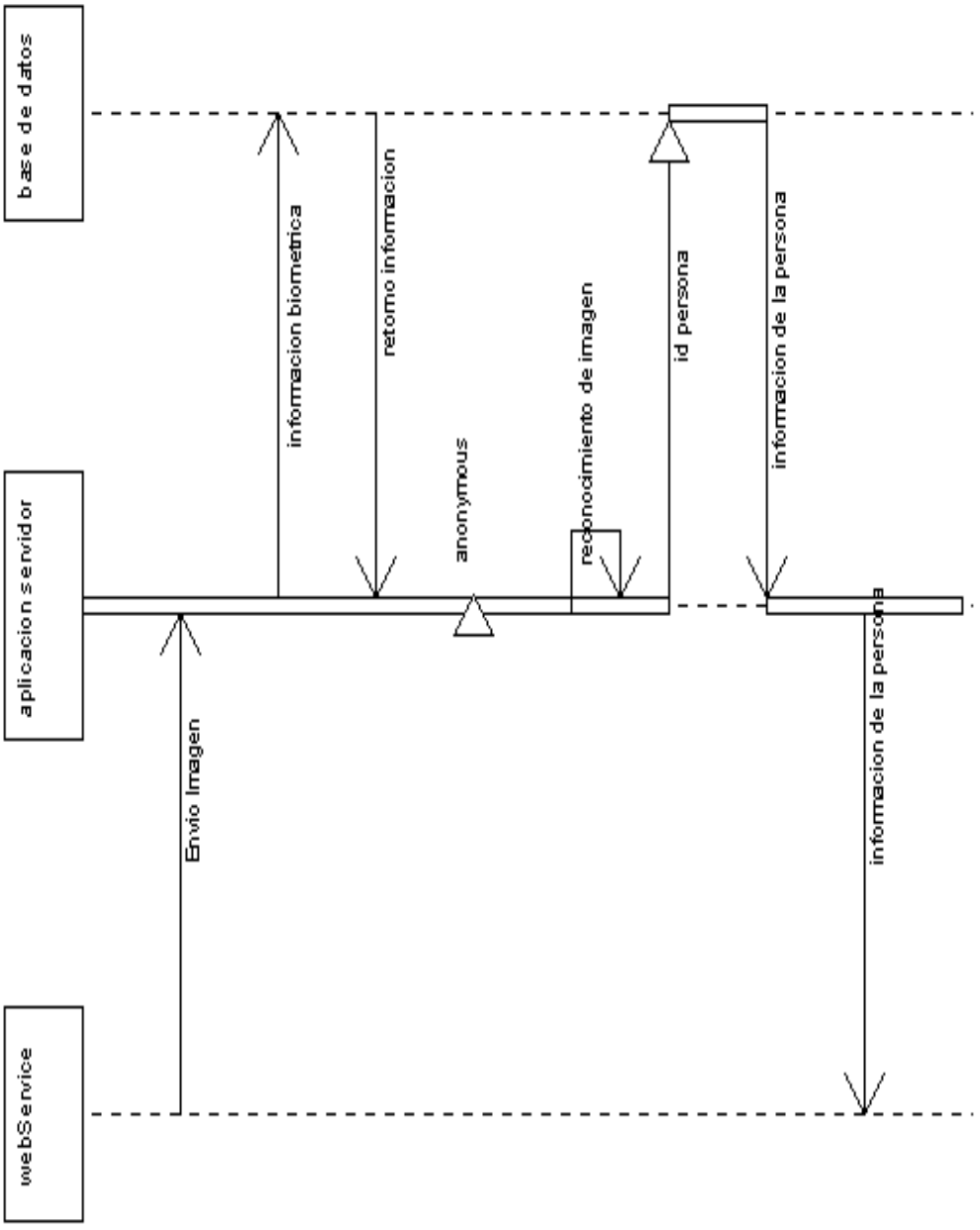
4.4.2.1 Diagrama de clases

Figura 8 Diagrama de clases etapa 2



4.4.2.2 Diagrama de secuencia

Figura 9 Diagrama de secuencia etapa 2



8.4.2.3 Requerimientos

Tabla 14 R-006 Conversión de tipos de imagen entre plataformas

Descripción	El sistema deberá tomar la imagen que reciba y transformarla en un tipo de imagen propio del sistema
Tipo	Interno
Entrada	Imagen recibida
Resultado	Imagen transformada

Tabla 15 R-007 Consulta de información biométrica en base de datos documental

Descripción	Permite al sistema consultar información biometría a la base de datos
Tipo	Interno
Entrada	id del usuario a consultar
Resultado	información biométrica retornada

Tabla 16 R-008 Consulta de información del individuo

Descripción	Permite al sistema consultar información de acceso en una base de datos relacional
Tipo	Interno
Entrada	id del usuario a consultar
Resultado	información de acceso retornada

Tabla 17 R-009 Consulta de información biométrica individuo

Descripción	Permite al sistema cuantificar las características faciales en la base de datos
Tipo	Interno
Entrada	no aplica
Resultado	información cuantificada de las características

Tabla 18 R-009 Almacenar información cuantificada

Descripción	Permite al sistema almacenar la información cuantificada en la base de datos
Tipo	Interno
Entrada	nombre del archivo de salida
Resultado	información cuantificada de las características guardadas de forma persistente, en formato XML con el nombre de archivo proporcionado

Tabla 19 R-010 Cargar información cuantificada

Descripción	Permite al sistema cargar en memoria la información cuantificada en la base de datos
Tipo	Interno
Entrada	nombre del archivo de entrada
Resultado	información cuantificada de las características cargada correctamente

Tabla 20 R-011 Realizar análisis por componentes

Descripción	Realiza un análisis a una imagen de sus características biométricas por medio del método PCA
Tipo	Interno
Entrada	Imagen a analizar
Resultado	Retorno de la información en forma de eigenvectores y eigenvalores

Tabla 21 R-012 Identificar persona

Descripción	Permite al sistema identificar a una persona en la base de datos por medio del metodoEigenface
Tipo	Interno
Entrada	Imagen de la persona a identificar
Resultado	Se identifico a la persona, o se retorno que la persona no se reconoce

Tabla 22 Caso de uso-007

Descripción	Permite al sistema Convertir un bitmap a un objeto de tipo java.awt.Imagen
Actores	Sistema
Precondiciones	Ninguna
Flujo norma	El sistema mapea correctamente el tipo de dato. El sistema crea un nuevo objeto de tipo imagen en base al bitmap.
Flujo alternativo	El sistema encuentra inconsistencias en la información y lo reporta
Pos-condiciones	Conversión del tipo de objeto realizada.

Tabla 23 Caso de uso-008

Descripción	Permite al sistema obtener la información facial de la base de datos
Actores	Sistema

Precondiciones	Debe existir información contenida en la base de datos
Flujo norma	El sistema crea una conexión con la base de datos El sistema realiza un query a la base de datos La base de datos envía la información al sistema El sistema mapea la información a una colección de objetos El sistema retorna la colección de objetos
Flujo alternativo	Si la base de datos no contiene información, entonces el sistema debe lanzar una excepción
Pos-condiciones	Se debe retornar la información contenida en la base de datos

Tabla 24 Caso de uso-009

Descripción	Permite al sistema reconocer las características faciales en la base de datos
Actores	Sistema
Precondiciones	Se debe tener una colección de imágenes
Flujo norma	Se analizan las imágenes por medio del método PCA Se identifican las distancias entre los rasgos mas característicos Se crea una matriz de objetos en la que se guarda la información recolectada
Flujo alternativo	n/a
Pos-condiciones	se reconocieron las características faciales

Tabla 25 Caso de uso-010

Descripción	Permite al sistema almacenar la información acerca de las características faciales de forma persistente en el servidor
Actores	Sistema
Precondiciones	reconocimiento de las características(PCA) de las imágenes de la base de datos realizado
Flujo norma	El sistema guarda la información aprendida en un XML
Flujo alternativo	n/a
Pos-condiciones	almacenamiento de la información realizada

Tabla 26 Caso de uso-011

Descripción	Permite al sistema almacenar la información acerca de las características faciales de forma persistente en el servidor
Actores	Sistema
Precondiciones	reconocimiento de las características(PCA) de las imágenes de la base de datos realizado
Flujo norma	El sistema guarda la información aprendida en un XML
Flujo alternativo	n/a

Pos-condiciones	almacenamiento de la información realizada

Tabla 27 Caso de uso-012

Descripción	Permite al sistema ejecutar el método Principal componentanalysis (PCA), por medio del cual se analizaran los componentes de una imagen
Actores	Sistema
Precondiciones	Ninguna
Flujo norma	Se trata a la imagen como un flujo de bytes Se identifica el promedio central Se identifica la desviación del promedio central Se halla la matriz de covarianza Se itera dicha matriz y se calculan los eigenvectores y los eigenvalores Se ordenan los eigenvectores y los eigenvalores
Flujo alternativo	si no se posee información en el XML, el sistema lanzara una excepción
Pos-condiciones	La información contenida en el XML debe ser retornada

Tabla 28 Caso de uso-013

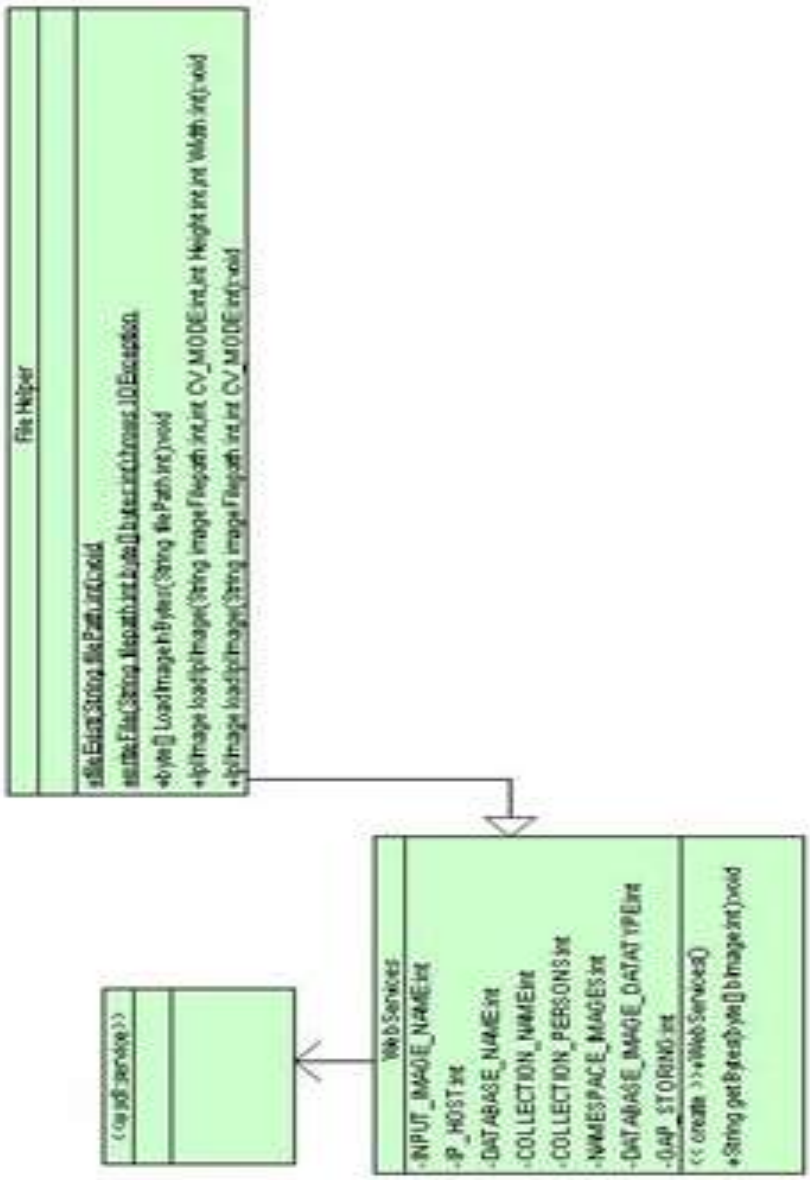
Descripción	Permite al sistema identificar a una persona dentro de la base de datos
Actores	Sistema
Precondiciones	Ninguna
Flujo norma	Se carga la información previamente recopilada en un XML Se analiza la información de la imagen a analizar por medio de PCA Se calculan las diferencias entre la imagen actual y las imágenes cargadas Se toma el id de la imagen con la menor diferencia Se busca en la base de datos la información de la persona con dicho ID Se retorna el objeto de una persona mapeado con la información contenida en la base de datos con el ID
Flujo alternativo	Si se detecta una diferencia menor a la de un porcentaje de certeza establecido, se retornara el objeto de una persona estática que representa una persona desconocida
Pos-condiciones	Se realizo el reconocimiento de la persona

4.4.3 Etapa tres - Web Service

En esta etapa se construirá el web service que comunicara el cliente android, con la lógica biometría en el lado del servidor.

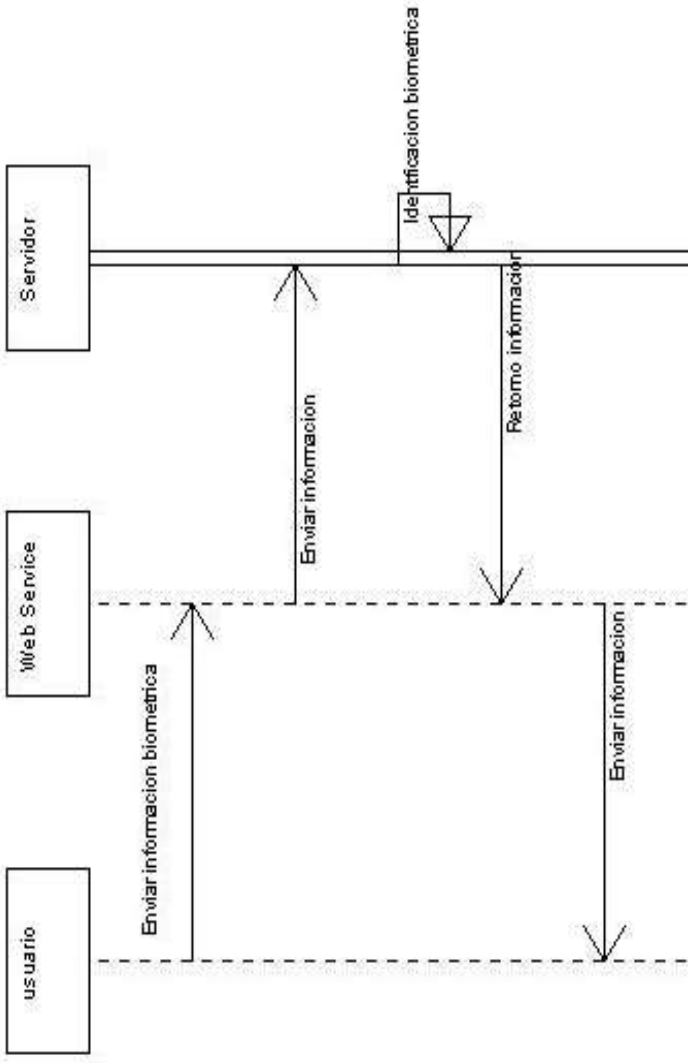
4.4.3.1 Diagrama de clases

Figura 10 Diagrama de clases etapa 3



4.4.3.2 Diagrama de secuencia

Figura 11 Diagrama de secuencia etapa 3



4.4.3.3 Requerimientos

Tabla 29 R-013 Recibir la información biométrica enviada desde el dispositivo móvil

Descripción	El sistema deberá tomar la imagen que reciba como un array de bytes
Tipo	Interno
Entrada	bytes representando la imagen recibida
Resultado	Imagen Recibida

Tabla 30 R-014 Usar el modulo de identificación

Descripción	El sistema deberá tomar la imagen que reciba y procesarla con el modulo de identificación
Tipo	Interno
Entrada	Imagen recibida
Resultado	información de la persona en la imagen

Tabla 31 R-015 Retorno de la información

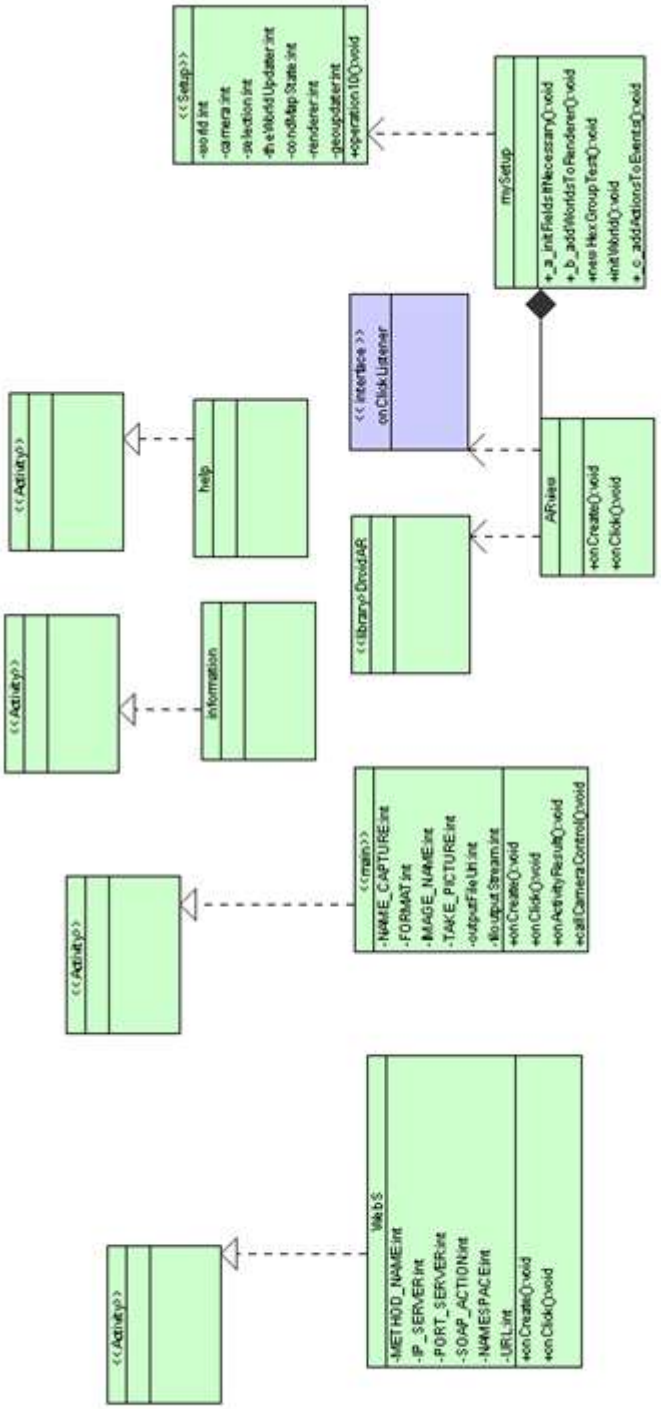
Descripción	El sistema deberá retornar la información procesada al dispositivo móvil
Tipo	Interno
Entrada	información
Resultado	información enviada

4.4.4 Etapa cuatro - Visualización de la información

En esta etapa se construirá la visualización de la información validada biométricamente.

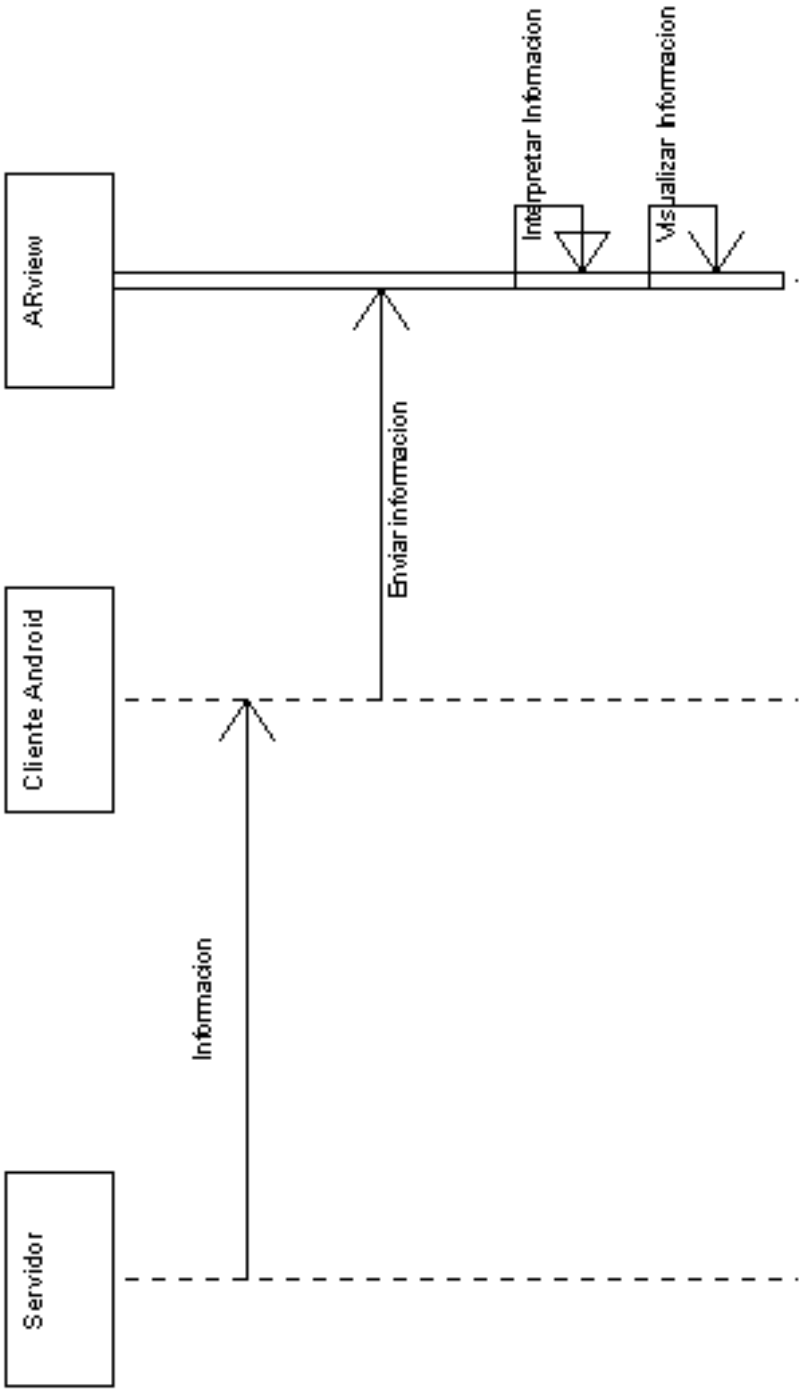
4.4.4.1 Diagrama de clases

Figura 12 Diagrama de clases etapa 4



4.4.4.2 Diagrama de secuencia

Figura 13 Diagrama de secuencia etapa 4



4.4.4.3 Requerimientos

Tabla 32 R-016 Recibir la información enviada desde el servidor

Descripción	El sistema deberá estar en la capacidad de recibir la información enviada desde el servidor
Tipo	Interno
Entrada	El nombre del sujeto El sexo del sujeto La edad del sujeto Los permisos que el sujeto posee
Resultado	información recibida

8.9. VALIDACION DEL PRODUCTO INTEGRO

Pruebas Unitarias: Las pruebas sobre el algoritmo de reconocimiento facial se dividieron en dos secciones, las pruebas con una base de datos facial de la universidad de Yale, y la segunda, con sujetos presentes dentro de un ambiente controlado .Los resultados fueron los siguientes:
Para la base de datos facial, el porcentaje de éxito fue del 95%, las veces en que el algoritmo no fue efectivo fue en los casos donde existía una iluminación mayor a las fotos contenidas en la base de datos.
Para las pruebas con sujetos en ambientes controlados, el porcentaje de éxito fue menor con un 85%, nuevamente la iluminación jugó un papel importante en las fallas, pero adicionalmente, la distancia y posición desde la cual se toma la foto también influyo.
Para mejorar el porcentaje de éxito se decidió almacenar 3 fotos del sujeto en diferentes posiciones, frontal, lateral derecho y lateral izquierdo, al realizar las pruebas el porcentaje de éxito fue mayor con un 89%

Pruebas de sistema:En estas pruebas se valido la el producto integro en sujetos presentes dentro de un ambiente controlado, los resultados de las pruebas fueron:

- Ajustar orientación cámara - Resultado: exitoso
- Activar la cámara - Resultado: exitoso
- Procesar imagen tomada- Resultado: exitoso
- Usar herramientas nativas - Resultado: exitoso
- Enviar información a servido - Resultado: exitoso
- Visualizar información de forma grafica - Resultado: exitoso
- Conversión de tipos de imagen entre plataformas - Resultado: exitoso
- Consulta de información biométrica en base de datos documental - Resultado: exitoso
- Consulta de información del individuo - Resultado: exitoso
- Consulta de información biométrica individuo - Resultado: exitoso
- Almacenar información cuantificada - Resultado: exitoso
- Cargar información cuantificada - Resultado: exitoso

- Realizar análisis por componentes - Resultado: exitoso
- Recibir la información
- biométrica enviada desde el dispositivo móvil - Resultado: exitoso
- Usar el modulo de identificación - Resultado: exitoso
- Retorno de la información - Resultado: exitoso
- Recibir la información enviada desde el servidor - Resultado: exitoso
- Recibir mensaje alterno en caso de no tener conexión - Resultado: exitoso
- Permitir repetir la captura de la información biométrica, de ser necesario - Resultado: exitoso

Figura 14 Capturas del programa cliente

La información es representada por medio de iconos, tal y como se aprecia en la imagen anterior, si se quiere obtener más información basta con presionar un icono para complementar la información, también se puede obtener información adicional seleccionando el nombre de la persona, de esta forma se muestra la información de una manera interactiva y amigable ante el usuario.

5. CONCLUSIONES

El desarrollo estuvo realizado principalmente en el lenguaje java, tardo 4 meses en implementarse, y al final se cuentan con dos aplicaciones, la primera corresponde al servidor de la aplicación, en el cual se corre el servicio que recibe la imagen, y por medio del algoritmo de biometría escogido, identifica la persona, y por último se retorna al cliente. La segunda corresponde a la aplicación móvil del cliente, esta se encarga de capturar la información biométrica, enviarla vía web services al servidor, y visualizar la respuesta de este, una vez se tenga la información del sujeto.

Se evidencia que efectivamente, es posible crear un prototipo con tecnologías libres para realizar la identificaciónbiométrica, con un buen porcentaje de éxito, sin embargo, el prototipo desarrollado solo es posible implementarlo en un ambiente controlado.
El uso de tecnologías libres es en gran medida, una buena manera de bajar los costos y además reducir el tiempo de desarrollo en un proyecto de software, sin duda, el prototipo desarrollado puede ser considerado como una tecnología libre, útil para construir un sistema robusto de seguridad.
Es posible realizar la inclusión de dispositivos móviles en sistemas de seguridad, incluso pueden ser parte esencial de este, su portabilidad y la facilidad de desarrollo en comparación a otros tiempos, lo hacen un dispositivo muy útil, incluso puede ser explotado en conjunto con otras aplicaciones que la empresa decida implementar.
Para una efectividad mayor, el algoritmo de reconocimiento facial debe ser mejorado, aplicando heurísticas, y técnicas para tratar el problema con la iluminación del ambiente, adicionalmente, y como es de suponerse, entre más fotos en distintas posiciones se tengan del sujeto,mayor será el porcentaje de éxito.

En base a la aplicación creada, es posible implementar un sistema robusto de seguridad, a continuación se enumeraran los requerimientos mínimos para implementar dicho sistema:

- Al menos un dispositivo móvil con android.
- Una infraestructura de intranet.
- Un servidor con capacidad para correr apache 5.5.

En el equipo servidor se instalara el web service, en dicho servidor puede existir o comunicarse (puede estar contenido en otro servidor) con la base de datos documental, básicamente la función de este servidor es responder a las peticiones de identificación biométrica que se hagan desde el cliente, por supuesto, el servidor debe tener conexión con la intranet. Aunque el sistema fue diseñado para trabajar en una intranet, es posible usarlo vía internet, sin embargo, en dado caso se deben aplicar métodos
de seguridad de comunicación adicionales. La base de datos, tal y como se comentaba en los alcances del proyecto, ya debe contener la información biométrica de los funcionarios, por eso sería conveniente desarrollar un sistema

para gestión de la información biométrica de dichos funcionarios. El cliente desarrollado se deberá instalar en el dispositivo móvil, la configuración sencillamente es indicar la IP del servidor, cabe aclarar que la información biométrica debe ser tomada en un ambiente controlado, con un fondo blanco, y de tal forma que se pueda apreciar la cara del funcionario en su totalidad, además, la distancia desde la cual se tomo la foto debe ser proporcional a la distancia de las fotos que residen en la base de datos. Es posible además desarrollar otros clientes, ya sean móviles o de escritorio, debido a la arquitectura del sistema, por lo tanto, podría incluso integrarse con el software ya disponible en la empresa como método de identificación alterno.

BIBLIOGRAFIA

Anil K. Jain, Patrick Flynn y Arun A. Ross, Handbook of Biometrics, Octubre 2007, Springer

CONDE VILDA, Cristina, Biometría. Reconocimiento facial mediante fusión 2D y 3D 2007, Dykinson, S.L. – Libros

PAJARES MARTINSANZ, Gonzalo Cruz Garca, Jesús M, Visión por Computador: Imágenes digitales y aplicaciones, 2001, Ra-Ma, Librería y Editorial Microinformática

PEKMAN Y W. FRIESEN, Facial Action Coding System, Eigenfaces vs. fisherfaces: recognition using class specific linear, 1978, Consulting Psychologist Press, Palo Alto

P. N. Belhumeur, J. P. Hespanha y D. J. Kriegman. IEEE Transactions on Pattern Analysis and Machine Intelligences, Julio 1997, pag 711–720.

SANCHEZ CALLE, Ángel, Aplicaciones en la visión artificial y la biometría informática, 2005, Dykinson, S.L.

Stockman, George; Shapiro, Linda G, Computer Vision, 2001, Prentice Hall

TAPIADOR MATEOS, Merino, tecnologías biométricas aplicadas a la seguridad, 2004 Editorial Microinformática.

THEODORIDIS, SERGIOS, Pattern Recognition, 2005, Elsevier Books.

Security management & assurance [online]<URL:http://csrc.nist .gov/groups /STM/index.html >

Smartphones growth exploding as Android operating system drives prices down[online].<URL:http://economictimes.indiatimes.com/tech/hardware/smartphones-growth-exploding-as-android-operating-system-drives-prices >