Propuesta para la implementación de un sistema facial biométrico de seguridad e identificación del personal que ingresa a las unidades militares para evitar la suplantación

Walter Ivan Borre Troncoso
Edgar Ramiro Parra Castañeda

Trabajo de grado para optar al título profesional:
Curso de Estado Mayor (CEM)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

2013

PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA FACIAL BIOMÉTRICO DE SEGURIDAD E IDENTIFICACIÓN DEL PERSONAL QUE INGRESA A LAS UNIDADES MILITARES PARA EVITAR LA SUPLANTACIÓN

MY EJC BORRE TRONCOSO WALTER IVAN
MY EJC PARRA CASTAÑEDA EDGAR RAMIRO
Curso CEM-2013

FUERZAS MILITARES DE COLOMBIA
ESCUELA SUPERIOR DE GUERRA
CURSO DE ESTADO MAYOR
Bogotá DC.
2013

PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA FACIAL BIOMÉTRICO DE SEGURIDAD E IDENTIFICACIÓN DEL PERSONAL QUE INGRESA A LAS UNIDADES MILITARES PARA EVITAR LA SUPLANTACIÓN

Trabajo de Grado

Asesor:

MY EJE BORRE TRONCOSO WALTER IVAN
MY EJC PARRA CASTAÑEDA EDGAR RAMIRO
Curso CEM-2013

FUERZAS MILITARES DE COLOMBIA
ESCUELA SUPERIOR DE GUERRA
CURSO DE ESTADO MAYOR
Bogotá DC.
2013

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

TITULO DEL PROYECTO

PROPUESTA PARA LA IMPLEMENTACIÓN DE UN SISTEMA FACIAL BIOMÉTRICO DE SEGURIDAD E IDENTIFICACIÓN DEL PERSONAL QUE INGRESA A LAS UNIDADES MILITARES PARA EVITAR LA SUPLANTACIÓN

INTRODUCCIÓN

El presente trabajo desarrollado bajo la metodología de investigación documental, permitió hacer una evaluación del sistema de seguridad actual del Ejército Nacional en cuanto al acceso a las unidades. Actualmente, y en las últimas dos décadas, las necesidades para contrarrestar las acciones de obtención de información, hurto de material y atentados terroristas han sido numerosas.

Sin embargo, uno de los problemas mas latentes ha sido la suplantación del personal militar, técnica utilizada por organizaciones armadas al margen de la ley para acceder a las unidades militares y obtener información de valor para la inteligencia militar la cual es usada posteriormente en contra de las unidades militares, convirtiendo el sistema en un factor de riesgo para el Ejército Nacional.

A raíz de esto, el presente trabajo presenta las ventajas de implementación de un mecanismo de identificación facial biométrico eficiente que se podría implementar al interior de las guardias y accesos de las unidades militares logrando garantizar la identidad del personal militar que por allí ingresa evitando la suplantación.

Para lograr este objetivo, este trabajo se desarrolla en tres capítulos: el primero, permitió identificar los tipos de tecnologías biométricas que existen, como funciona el sistema, de que se compone y que se pueden ajustar a las necesidades del Ejército. Segundo, se analiza el sistema de seguridad actual con un sistema biométrico facial, ampliando el funcionamiento y ventajas que tiene el sistema. Finalmente, se hace determinante como se puede implementar un sistema biométrico facial con la información que cuenta actualmente el Ejército Nacional.

1. PROBLEMA DE INVESTIGACIÓN

Descripción:

A través de la historia en Colombia durante los dos últimos siglos, ha sido evidente la intensión de las organizaciones al margen de la ley por propiciar duros golpes a las Fuerza Militares a través de múltiples mecanismos, empleando diversos métodos para la obtención de información, hurto de material y atentados terroristas.

Uno de esos mecanismos es la suplantación de personal militar, mediante el uso de prendas, distintivos e identificaciones militares, con lo cual los integrantes de estas organizaciones buscan acceder a las unidades militares para obtener información de valor para la inteligencia militar y para estas organizaciones, empleándola el desarrollo de actividades terroristas y de sabotaje contra las unidades militares, convirtiendo esta actividad en una vulnerabilidad y factor de riesgo para la seguridad de las unidades militares y sus integrantes.

Los diferentes mecanismos de control instalados por las diferentes unidades han jugado un papel muy importante como medio de contención y mitigación de este riesgo logrando en muchos casos la detección de integrantes de organizaciones armadas al margen de la ley intentando acceder a las diferentes unidades, sin embargo, esta detección de suplantadores no siempre ha sido posible tempranamente. Las organizaciones al margen de la ley día a día buscan mecanismos que les permitan ser más eficientes en esta tarea y aprovechando la gran cantidad de personal con que cuentan las Fuerzas Militares y la escasa capacidad para acceder a las bases de datos y lograr una plena identificación se permean los filtros y dispositivos con los que cuentan actualmente las unidades militares.

Los argumentos anteriores permiten evidenciar una falencia en las medidas de seguridad que actualmente poseen las guardias y accesos a las unidades militares y a la vez representan una oportunidad latente para las organizaciones al margen de la ley ya que no existe un mecanismo que permita constatar en tiempo real la autenticidad de la identificación.

Para contrarrestar esta vulnerabilidad, algunas unidades han desarrollado ciertas iniciativas, tendientes a identificar al personal que labora en las unidades con mecanismos de identificación biométrica (lector de huella y lector de iris), pero esta estrategia hasta el momento no ha sido muy eficiente ya que las bases de datos que poseen son limitadas y corresponden a las que las unidades cargan, sin poder realizar una comprobación del personal externo que pretende visitar la unidad, esta medida ha resultado eficaz en unidades donde el ingreso es mínimo y totalmente restringido, para unidades con altos flujos de ingreso no es muy factible ni eficiente.

Formulación:

¿Qué mecanismo de identificación facial biométrico eficiente se podría implementar al interior de las guardias y accesos de las unidades militares logrando garantizar la identidad del personal militar que por allí ingresa evitando la suplantación?

2. OBJETIVOS

2.1 GENERAL

Proponer la implementación de un sistema modelo de seguridad e identificación facial biométrico, que permita establecer en tiempo real la identidad del personal militar del Ejército Nacional que ingresa a las unidades militares para evitar la suplantación.

2.2 ESPECÍFICOS

2.2.1 Identificar los tipos de tecnologías biométricas que existen y estudiar cual se ajusta a las necesidades de las unidades militares del Ejército Nacional

2.2.2 Establecer la compatibilidad o incompatibilidad de los sistemas de seguridad ya existentes con un sistema de identificación facial biométrico

2.2.3 Determinar cuál sería el tipo de información y recursos necesarios para adoptar un sistema de identificación facial biométrico.

3. JUSTIFICACIÓN

Dado el desarrollo del conflicto armado interno en Colombia y el intento de los grupos al margen de la ley de instaurar dentro de sus planes delictivos los pasos contemplados en la guerra popular prolongada y la lucha por todos los medios, incorporando en estos el terrorismo y ataque a las unidades militares como una herramienta más de su actividad delictivo; estos grupos han realizado suplantación de las Fuerzas Militares de forma individual (19 OCT 06 atentado a la Universidad Militar, 27 MAR 13 en el Universidad Militar Nueva Granada) y colectiva (26-JUL01 secuestro en el edificio Miraflores de Neiva, 11ABR 02 secuestro de los diputados del Valle, 27 FEB 06 asesinato de los concejales de Rivera (Huila), 21 DIC 09 secuestro y asesinato del gobernador del Caquetá), que han sido de renombre a nivel nacional, lo cual ha alertado a las unidades militares sobre este nuevo modus operandi.

El avance del arte militar en el mundo y la aplicación de nuevas tecnologías en la ejecución de la guerra, han estimulado al Ejercito Nacional en la modernización de la Fuerza, consolidándola como una fuerza armada regular acorde con las necesidades y expectativas de la modernidad, favoreciendo con ello la legitimidad de la institución ante la población civil y la comunidad internacional.

A través del régimen interno en las unidades, se regulan las actividades dentro de la misma, y se efectúan las distribuciones de las funciones de cada uno de los miembros de la unidad táctica. Adicionalmente se establecen las ordenes en cuanto al manejo de personal, servicios de guarnición, sistemas de seguridad y desarrollo de controles para la verificación de la gestión.

De acuerdo al Reglamento de régimen interno para unidades tácticas del Ejercito Nacional, se dan actualmente las pautas para un estricto cumplimiento

para el personal tanto militar como civil. Para el caso especifico de seguridad en las unidades militares, se cumple con el reglamento de servicio de guarnición. Este, establece las normas y procedimientos que deben cumplir los comandos, unidades y personal de las Fuerzas Militares en el desarrollo de sus actividades específicas de guarnición.

La responsabilidad de las normas de seguridad que actualmente se cumplen en las guardias del Ejército Nacional recaen inicialmente sobre los jefes de las secciones de contrainteligencia, quienes son los encargados de emitir normas de seguridad y tienen bajo responsabilidad la seguridad de las instalaciones bajo las cuales se encuentran orgánicos, además delos comandantes de guardia, los cuales en su mayoría no cuentan en sus lugares de trabajo con tecnología que soporte la información que se requiere para lograr una plena identificación del personal militar.

Dentro de los procesos generales se encuentra: la revisión de vehículos, verificando la identidad de los ocupantes; inspección de paquetes; identificación del personal mediante el fichero y fecha de vencimiento; el comandante de guardia o Cabo de guardia deben ser quienes atienden al personal y autorizan su ingreso; las personas que ingresan de visita en algunas unidades quedan registrados en una base de datos e ingresan con ficheros de visitantes; entre otros. Este proceso genera que los accesos a las unidades sea bajo los criterios de los servicios de la Guardia, haciendo vulnerable el sistema de seguridad para intenciones delictivas y terroristas.

Por consiguiente es necesario que bajo medidas de contrainteligencia, el Ejercito Nacional, adopte todas aquellas medidas activas y pasivas encaminadas a prevenir, detectar y neutralizar la acción de los sistemas de inteligencia de enemigos actuales y potenciales, con el objeto de proteger el personal de la subversión; las instalaciones y material del sabotaje y la información del espionaje.

4. MARCO DE REFERENCIA

4.1 MARCO DE ANTECEDENTES TEMÁTICOS DE LA INVESTIGACIÓN

La biometría es un método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento. Se trata de un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a sus congéneres por su aspecto físico, su voz, su forma de andar, etc.

En el contexto tecnológico, la biometría expresa la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad (Travieso, 2011).

En la actualidad, la tecnología ha permitido automatizar y perfeccionar estos procesos de reconocimiento biométrico, de forma que tienen una variedad de aplicaciones (iris del ojo, el calor facial, la voz, la mano o la firma) y finalidades, demostrando así que es uno de los mejores métodos de identificación humana.

Los antecedentes de la tecnología biométrica aplicados a la seguridad de acuerdo a Pérez (2011) se desarrollarlo de la siguiente forma:

> Los primeros antecedentes de los que se tiene referencia sobre la biometría datan de hace más de mil años en China, donde los alfareros comenzaron a incluir sus huellas dactilares en los productos que realizaban como símbolo de distinción o firma, lo que les permitía diferenciarse del resto.
> Sin embargo, no fue hasta finales del siglo XIX cuando Alphonse Bertillon – antropólogo francés que trabajó para la policía– comenzó a dar a la biometría el carácter de ciencia, profesionalizando su practica. Basaba su teoría en que una cierta combinación de medidas del cuerpo humano era invariable en el tiempo, lo que permitió dar solución al problema de identificar a los criminales convictos a lo largo de toda su vida.

El sistema de Bertillon o "Antropometría", que incluía, entre otras, medidas como el largo y ancho de la cabeza o la longitud del pie izquierdo y del antebrazo, se comenzó a utilizar comúnmente a lo largo de todo el mundo. Sin embargo, su efectividad se puso en duda al presentarse algunos problemas en el uso de diferentes medidas y, especialmente, por las dificultades en la diferenciación de sujetos extremadamente similares como los gemelos.

Esta desacreditación hizo que Sir Edward Henry, Inspector General de la Policía de Bengala, buscase otras técnicas y se interesase por las investigaciones de Sir Francis Galton, el cual utilizaba la huella dactilar como método de identificación. Primero en Bengala y posteriormente en Londres (1901), Sir Edward Henry estableció su oficina de huella dactilar exitosamente y consiguió rápidamente la aceptación de la comunidad a nivel mundial. Así, los métodos utilizados en oriente desde siglos atrás fueron introducidos exitosamente en occidente.

Ya a comienzo de los años 70, Shearson Hamil, una empresa de Wall Street, instaló Identimat, un sistema de identificación automática basado en huella dactilar que se utilizó para el control de acceso físico a instalaciones, siendo la primera solución biométrica de uso comercial. Desde entonces se ha investigado mucho en el campo de la biometría, detectándose multitud de rasgos biométricos diferentes a la huella dactilar (p.22-23).

La importancia de un sistema de identificación personal biométrico radica en resolver la identidad de una persona basada en dos planteamientos: reconocimiento y verificación. El reconocimiento determina la identidad de una persona dentro de un conjunto conocido de identidades y la verificación confirma o niega la identidad aducida por una persona.

De acuerdo a Pérez C. (n.d) existen dos modos fundamentales de funcionamiento para un sistema de reconocimiento basado en parámetros biométricos: Verificación: El usuario se identifica mediante un método típicamente

no biométrico, como un código (PIN) o una tarjeta, y se ha de comprobar (verificar) que la identidad proporcionada es correcta. Identificación: Se trata de averiguar la identidad del sujeto buscando en una base de datos una representación de parámetros biométricos que se corresponda con la lectura del sistema.

Para Travieso (2011) "Una verificación certera de la identidad de una persona podría disuadir la delincuencia y el fraude, dinamizar las transacciones comerciales y salvaguardar los recursos críticos".(p.8)

Las características que puede utilizar un sistema biométrico determinan la identidad de una persona (tanto físicas como psicológicas), entre los criterios que se pueden analizar con este tipo de sistemas se encuentran (Hernández, 2010):

- Universalidad, indica como de común es encontrar esta característica en todas las personas u objetos a reconocer.
- Carácter distintivo, indica si dicha propiedad, es suficientemente diferente entre un conjunto de personas u objetos diferentes.
- Permanencia, indica la estabilidad en el tiempo de dicha característica.
- Colectividad, indica si la característica es fácilmente adquirida y medida por el sistema.
- Rendimiento, indica la precisión, velocidad y coste (recursos) necesarios para llevar a cabo el reconocimiento.
- Aceptabilidad, indica en que medida está la gente preparada para aceptar el uso de esta técnica.
- Elusión, indica la respuesta del sistema cuando alguien está tratando de Engañarlo

De acuerdo a lo anterior el reconocimiento facial se destaca por ser una técnica de alta capacidad de respuesta frente a múltiples características biométricas lo que lo hace útil para el desarrollo de aplicaciones no intrusivas. Dentro de los principales métodos de reconocimiento facial se encuentran los

rasgos locales (ojos, nariz, boca, distancias y ángulos de la cara), globales (información de toda la cara) y mixtos.

La aplicación de la biometría facial se ha dado en tres grupos principales: el primero es a nivel comercial, aplicaciones para ordenadores, seguridad electrónica, acceso a internet, tarjetas de crédito, controles de acceso teléfonos móviles entre otros.

> La empresa Interbank anunció el comienzo de la prueba piloto de un sistema de reconocimiento facial en sus cajeros en Perú, convirtiéndose en el primer banco a nivel mundial en evaluar esta tecnología para llevar a un siguiente nivel la seguridad en los servicios financieros y así evitar el fraude por suplantación de identidad. El sistema se pone en marcha cada vez que un cliente desea hacer operaciones en un cajero automático, éste captará una imagen de su rostro y la validará para confirmar que corresponda al usuario registrado con el número de tarjeta ingresado y clave secreta correspondiente. (Pruebas piloto de reconocimiento facial en cajeros)

En segundo lugar, se encuentra el uso gubernamental, en procesos de identificación para documentos de identidad, seguridad social, controles en aeropuertos, fronteras entre otros. En este campo, en Colombia, actualmente la Registraduría Nacional del Estado Civil, ha implementado un sistema de identificación biométrica para los procesos electorales:

> Actualmente el AFIS de la Registraduría Nacional del Estado Civil de Colombia almacena más de 740 millones de huellas dactilares de colombianos, desde 1952 a la fecha, incluyendo no sólo a los mayores de edad sino también a los jóvenes mayores de 14 años que cuentan con tarjeta de identidad biométrica, y los varios juegos de huellas de quienes en algún momento han tramitado duplicados o rectificaciones de sus documentos.

El AFIS permite hacer búsquedas 1 a 1, para cotejar que la huella de una persona sí corresponde efectivamente a su titular, al comparar la huella con la información encriptada de la cédula de ciudadanía o con la información que reposa en las bases de datos de la Registraduría Nacional, y búsquedas 1 a N, para determinar entre el universo de datos a quién corresponde una huella determinada.

La principal característica del sistema de identificación colombiano es que la base de datos AFIS se comunica con la base de datos de registro civil, que contiene información del nacimiento, matrimonio y defunción de todos los colombianos. Por ello es posible que a partir de una huella dactilar, o incluso un fragmento de una huella, se pueda identificar no sólo a la persona a quien pertenece sino adicionalmente obtener los principales datos biográficos de ese colombiano.

Se trata de un AFIS civil, que contiene información de todos los colombianos mayores de 14 años, lo cual marca una diferencia fundamental con las bases de datos de otros países, que tienen AFIS criminal ya que reseñan únicamente a personas con antecedentes penales o a los inmigrantes. (Sánchez, 2011)

Finalmente, el otro grupo de aplicación biométrico es en el campo forense, para investigaciones criminales, identificación de cadáveres y personas desaparecidas.

La debilidad principal de las técnicas convencionales, tales como el uso de tarjetas magnéticas, números de identificación personales (PINs) y contraseñas, es que los medios de autenticación y acceso son vulnerables a ser hurtados y utilizados por otra persona que finja ser uno mismo. La identificación por biometría contrarresta el riesgo de robo de identidad, ya que cada individuo, con o sin otro método de identificación necesario (por ejemplo, una tarjeta), debe probar al sistema que es quien dice ser. Esto se logra corroborando características irrepetibles del individuo (iris, voz,

huellas dactilares, rostro, etc.) con una base de datos digital. (Ventajas de la autenticación biométrica, n.d)

Durante lo últimos años, se han hecho estudios de técnicas de reconocimiento facial y se han abarcado áreas como la inteligencia artificial y biología. La industria de tecnología biométrica constantemente desarrolla nuevos componentes, modelos de identificación y clasificación de rasgos del comportamiento, lo que hace que la biometría se presente como una de las mejores opciones para reconocer o autenticar a las personas.

4.2 MARCO CONTEXTUAL

La seguridad militar se constituye en el conjunto de medidas activas y pasivas de contrainteligencia con carácter preventivo, encaminadas a garantizar la integridad de la institución militar, el cumplimiento de la misión y el ejercicio del mando para proteger cualquier tipo de amenaza al personal contra la subversión, la información contra el espionaje y las instalaciones, material y equipos del sabotaje.

La clasificación de la seguridad de acuerdo al Manual de Seguridad Militar (2009) es: seguridad física, seguridad operacional, seguridad de personal, seguridad técnica y seguridad en la información y documentación. Para el desarrollo de este trabajo, se tendrá en cuenta la seguridad física, definida como:

> Seguridad Física: estudia los diferentes aspectos relacionados con la protección de personas, bienes e instalaciones, los riesgos que pueden atentar contra su integridad y las técnicas que se utilizan para prevenir y controlar dichos riesgos. Conjunto de medidas previstas, planeadas y aplicadas para detectar oportunamente la aproximación de personas o elementos hostiles y mantenerlos fuera de las instalaciones propias. Sirve de base para la seguridad de personal y la seguridad de información. (Capitulo 1)

Este trabajo va dirigido a fortalecer los mecanismos de seguridad, empleados en las guardias del Ejército para evitar la suplantación.

Se presenta a la Central de Contrainteligencia Militar (CECIM), cuya misión es adoptar las medidas activas y pasivas encaminadas a prevenir, detectar y neutralizar la acción de los sistemas de inteligencia enemigos actuales y potenciales para proteger al personal de la subversión, a las instalaciones y material de sabotaje, así como a la información del espionaje.

La misión central de CECIM, es producir la contrainteligencia del Ejército a nivel Nacional en apoyo a operaciones militares mediante la prevención, detección y neutralización de las amenazas internas y externas, con el fin de garantizar la integridad de la Fuerza.

Figura 1 Organigrama CECIM

Fuente: Central de Contrainteligencia Militar. CECIM

Las actividades de la central de contrainteligencia militar están encaminadas en generar estrategias de neutralización en operaciones y prevención como lo muestra el siguiente gráfico:

Figura 2 Estrategia de Neutralización

Figura 3 Estrategia de Prevención

Fuente: Central de Contrainteligencia Militar 2010. CECIM

La implementación de un sistema de seguridad facial biométrico para las Unidades Militares del Ejército Nacional, contribuirá con la visión y capacidades que tiene la Central de Contrainteligencia Militar CECIM.

Visión:

La central de contrainteligencia del ejército se proyecta como una unidad en continua actualización profesional, técnica y científica, preservando los principios y valores institucionales para actuar con anticipación frente a la corrupción, neutralizando el accionar de la amenaza.

4.3 MARCO LEGAL O NORMATIVO:

La seguridad militar debe entenderse como la efectiva y apropiada protección no sólo de una Unidad Militar, sino además de los elementos que la componen, tales como las persona, la información, la documentación, las instalaciones, los elementos técnicos y en sí la Misión Constitucional encomendada; se fundamenta en la responsabilidad de las personas involucradas, el entrenamiento recibido y el respeto por los Derechos Humanos y el Derecho Internacional Humanitario, de todos aquellos con los que se interrelacionen los miembros de la Institución Militar en cumplimiento de su misión Constitucional.

Articulo 2: Son fines esenciales del Estado: servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo.

Las autoridades de la República están instituidas para proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los

de comportamiento, propias y únicas del individuo, conocidas como autentificadores. (Espinosa, n.d)

FAR (False AcceptanceRate): Porcentaje de personas no autorizadas aceptadas por el sistema.

FRR (False RejectRate): Porcentaje de personas autorizadas no aceptadas por el sistema.

SR (SuccessRate): Responde a una combinación de los dos factores anteriores que se utiliza como indicador de la resolución total del sistema.

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.

MÉTODO DE INVESTIGACIÓN

5.1 TIPO DE INVESTIGACIÓN

Para el desarrollo del presente trabajo, se determinaron los principales tipos de tecnologías biométricas y como ha sido su aplicación en temas de seguridad, los cuales pueden contribuir a mejorar las normas y procedimientos de seguridad en las unidades militares del Ejercito Nacional.

Para lograr este propósito, este trabajo se desarrolló bajo la metodología de investigación documental que es definida por Eyssautier (2006) como: "aquella que depende exclusivamente de fuentes de datos secundarios, o sea, aquella información que existe en documentos y materiales de índole permanente y a la que se puede acudir como fuente de referencia en cualquier momento y lugar sin

alterar su naturaleza o sentido para poder comprobar su autenticidad. Estos datos se encuentran en las bibliotecas públicas o en Internet (p.159)

De acuerdo a los tipos de investigación documental y de acuerdo al trabajo de investigación desarrollado, la información obtenida para su análisis, se encuentra dentro del tipo de investigación documental informativa definida como: "una panorámica acerca de la información relevante de diversas fuentes confiables sobre un tema específico, sin tratar de aprobar u objetar alguna idea o postura. Toda la información presentada se basa en lo que se ha encontrado en las fuentes." (Técnicas de la investigación).

5.2 DISEÑO METODOLÓGICO

Para lograr el propósito de este trabajo, se hizo una investigación en documentos especializados y actualizados que permitieron identificar los diferentes tipos, tecnologías y aplicaciones que se han dado en el área de la biometría.

Esta información permitió hacer un análisis sobre la situación actual de los controles de verificación y gestión del personal tanto que labora en el Ejercito Nacional, como del personal externo que tiene acceso a las diferentes unidades; e identificar cuales de los mecanismos tecnologías de seguridad que brindan los sistemas de biometría facial se adoptan a las necesidades del Ejercito Nacional contribuyendo a prevenir, detectar y neutralizar la acción de los sistemas de inteligencia de enemigos actuales y potenciales, con el objeto de proteger el personal de la subversión; las instalaciones y material del sabotaje y la información del espionaje.

El diseño metodológico utilizado, esta basado en un análisis de doctrina (Guía Metodológica de Investigación, 2013) ya que la información aquí analizada contribuye para que el Ejército Nacional guíe las acciones y neutralice todos aquellos aspectos que van en detrimento de los intereses nacionales. Este

proyecto tiene el propósito de generar la información, difundirla, aplicarla y actualizarla.

5.3 OBJETO DE ESTUDIO

Analizar los diferentes tipos de tecnología biométrica facial y su aplicación a la seguridad que permitan presentar al Ejército Nacional un proyecto con la información y recursos necesarios para poder adoptar un sistema de identificación biométrico facial en las unidades del Ejército Nacional.

5.4 INSTRUMENTO PARA LA COLECTA DE DATOS

A través del análisis documental también conocido como análisis de fuentes secundarias, se seleccionaron y analizaron todos aquellos documentos que contenían la información relacionada con el objeto de estudio.

De acuerdo a Martín (2009), el análisis documental se puede definir como el conjunto de operaciones (unas técnicas y otras intelectuales) que se realizan para representar tanto la forma como el contenido de documentos primarios, generando de esta forma otros documentos secundarios cuyo objetivo no es otro que facilitar al usuario la identificación precisa y recuperación posterior de los documentos primarios representados

Este instrumento de recolección de datos, permitió identificar todos los aspectos contextuales existentes a nivel mundial sobre los diferentes tipos de tecnología biométrica facial usadas. La mayor parte del soporte de información documental recolectado pertenece a documentación electrónica y a documentos institucionales del Ejército Nacional.

6. ANALISIS DE LA INFORMACIÓN

La información utilizada en el desarrollo de este trabajo corresponde al análisis de la información relacionada con los sistemas faciales biométricos utilizados específicamente para temas de seguridad.

Actualmente, en Colombia, el sistema biométrico utilizado es el de la huella dactilar, sin embargo, la consulta y análisis de la información permitió ampliar un poco mas el concepto sobre las diferentes tecnologías de biometría y como son utilizadas en los sistemas de seguridad.

Actualmente, no existe un sistema unificado de identificación y acceso a las unidades del Ejército Nacional, en un 99% la identificación se hace a través de un documento de identificación que es vulnerable de falsificar, lo cual pone en riesgo a las unidades.

La información obtenida sobre el tema de la biometría facial fue sometida a análisis y clasificación lo que nos permitió estructurar el desarrollo del trabajo, identificando las diferentes tecnologías, posteriormente como se comparan y que pueden aportar a los sistemas actuales de seguridad en las unidades y finalmente se presenta una propuesta de cual debería ser el sistema mas adecuado de ingreso a las unidades y que se necesitaría para su implementación.

6.1 MATRICES REVISIÓN DOCUMENTAL

TEMA DE INVESTIGACIÓN: Propuesta para la implementación de un sistema facial biométrico de seguridad e identificación del personal que ingresa a las unidades militares para evitar la suplantación.

FUENTE DOCUMENTAL	JUSTIFICACIÓN
Travieso, C.M., del Pozo, M. Y Ticay, J.R (2011). Sistemas Biométricos. Las Palmas, España: Universidad de las Palmas de Gran Canaria.	La información contenida en este documento, permite identificar la definición de biometría, porque se debe usar, su funcionamiento básico y las tecnologías existentes. Punto de partida para la comprensión e identificación de los sistemas biométricos, tema de investigación
Hernández, R.G. (2010) Estudio de técnicas de reconocimiento facial. Barcelona, España: Universidad Politécnica de Cataluña.	Este documento, presenta los diferentes sistemas biométricos, sus funcionalidades y como se comporta el uso de estas técnicas en los diferentes mercados.
Pérez, P., Álvarez, E., De la Fuente, S., y García, L. (2011). Estudio sobre las tecnologías biométricas aplicadas a la seguridad. Madrid, España: Instituto Nacional de Tecnologías de la Comunicación (INTECO)	Este documento, presenta todos los antecedentes, conceptos claves, tipos, técnicas, análisis, beneficios entre otros de la aplicación de las técnicas de biometría aplicadas específicamente a la seguridad. Este documento se presenta como punto de partida para justificar la implementación de un modelo biométrico en las unidades del Ejército, tema principal de la investigación.

Pérez, P., Álvarez, E., De la Fuente, S., y García, L. (2011). Guía sobre las tecnologías biométricas aplicadas a la seguridad. Madrid, España: Instituto Nacional de Tecnologías de la Comunicación (INTECO)	Este documento permitió identificar las diferentes características y tipologías biométricas, sus usos y aplicaciones, los beneficios y la gestión de riesgos. Información determinante para el tema de investigación.

2. División de las fuentes de información

INFORMACIÓN PRIMARIA	INFORMACIÓN SECUNDARIA
Travieso, C.M., del Pozo, M. Y Ticay, J.R (2011). Sistemas Biométricos. Las Palmas, España: Universidad de las Palmas de Gran Canaria.	Pérez C, J.C., y Paredes, R. (n.d) Sistemas de seguridad basados en características biométricas. Extraído el 24 de Marzo de 2013 desde http://www.iti.es/media/about/docs/tic/07/2005-06-biometria.pdf
Hernández, R.G. (2010) Estudio de técnicas de reconocimiento facial. Barcelona, España: Universidad Politécnica de Cataluña.	Pruebas piloto de reconocimiento facial en cajeros (n.d). Extraído el 24 de Marzo de 2013 desde http://biometria.smartmatic.com/category/reconocimiento-facial
Pérez, P., Álvarez, E., De la Fuente, S., y García, L. (2011). Estudio sobre las tecnologías biométricas aplicadas a la seguridad. Madrid, España: Instituto Nacional de Tecnologías de la Comunicación (INTECO)	Sánchez, C.A. La experiencia colombiana en identificación biométrica aplicada a las elecciones. Extraído el 24 de Marzo de 2013 desde http://www.registraduria.gov.co/-Biometria-.html

Pérez, P., Álvarez, E., De la Fuente, S., y García, L. (2011). Guía sobre las tecnologías biométricas aplicadas a la seguridad. Madrid, España: Instituto Nacional de Tecnologías de la Comunicación (INTECO)	Sirovich, L. y Kirby, M. (1987) A Low-Dimensional Procedure for the Characterization of Human Faces. J. Optical Soc. Am. A. Vol. 4, No.3. Extraído el 19 de junio desde http://www.biometria.gov.ar/metodos-biometricos/facial.aspx
	Ventajas de la autenticación biométrica (n.d). Extraído el 24 de Marzo de 2013 desde http://biometria.smartmatic.com/ventajas-de-la-autenticacion-biometrica

3. Información que sirve para determinar conceptos:

INFORMACION DE CONCEPTUALIZACIÓN	INFORMACIÓN DE RELACIÓN	INFORMACIÓN DE COMPARACIÓN
Sistema actual de seguridad en el Ejército Nacional Sistema biométrico facial Beneficios de un sistema biométrico	Sistemas biométricos existentes y aplicaciones a la seguridad	Sistemas biométricos vs Aplicación de sistemas de seguridad en el Ejército Nacional de Colombia

4. Datos más relevantes de la revisión documental

CATEGORÍAS TEMÁTICAS CENTRALES	CATEGORÍAS PERTINENTES	SUBCATEGORIAS PERTINENTES
Tipos de tecnologías biométricas existentes que se ajustan a las necesidades de las unidades militares del Ejército Nacional Compatibilidad o incompatibilidad de los sistemas de seguridad existentes con un sistema de identificación facial Información y recursos necesarios para adoptar un sistema de identificación biométrico	Sistemas biométricos fisiológicos Sistemas biométricos de comportamiento Criterios para definir un sistema biométrico Reconocimiento de imágenes fijas Principales técnicas Métodos utilizados	Beneficios de implementar un sistema de identificación facial biométrico Casos de éxito

7. DIAGNOSTICO

La información seleccionada y analizada para este trabajo, permitió identificar las diferentes tecnologías biométricas existentes, los equipos usados, los beneficios y/o contras para los sistemas de seguridad.

Posteriormente, se hizo un análisis de la situación, procedimientos e información actual de los sistemas de seguridad utilizados por el Ejército Nacional para hacer una comparación con los usos y aplicaciones que tienen los sistemas de tecnología biométricos así como de sus beneficios.

Sin embargo se identifico que el Ejercito Nacional, basa su sistema de seguridad e ingreso a las unidades a través de los procedimientos que tienen los comandantes de guardias. El 99% de los casos la identificación se hace a través del documento de identidad, lo que hace totalmente vulnerable el sistema a la suplantación y falsificación de documentos, poniendo en riesgo a la institución.

En Colombia no existe un sistema biométrico de identificación facial, por lo cual no se puede establecer compatibilidad o incompatibilidad con los sistemas existentes, sin embargo se hizo un análisis de los sistemas de identificación biométrica facial, su uso y beneficios que podría traer para el sistema de seguridad en las unidades.

De esta forma fue posible determinar un mecanismo de identificación eficiente que se podría implementar al interior de las guardias y accesos de las unidades militares logrando garantizar la identidad del personal militar que por allí ingresa evitando la suplantación.

8. PROPUESTA DE INTERVENCIÓN

8.1 TIPOS DE TECNOLOGÍAS BIOMÉTRICAS EXISTENTES QUE SE AJUSTAN A LA NECESIDAD DE LAS UNIDADES MILITARES DEL EJERCITO NACIONAL.

En un contexto tecnológico, "la biometría expresa la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad" (Travieso, 2011). Las labores de biometría se realizan de forma automática y sus técnicas se utilizan para medir características físicas o de comportamiento de las personas con el objetivo de establecer una identidad.

Dentro de los métodos de identificación mas eficaces se encuentran los que están basados en la colección de rastros dactilares y las muestras de acido desoxirribonucleico (ADN). Sin embargo como sistema práctico y seguro de identificación se utiliza la huella dactilar y ahora se utilizan otros rasgos morfológicos para identificación como son el iris del ojo, el calor facial, la voz, la mano o la firma.

Dentro de las ventajas de utilizar un sistema biométrico se encuentra la facilidad de uso, ya que se evita el uso de elementos externos a la hora de la identificación. En un sistema biométrico el usuario no tiene que recordar, no tiene que cambiar nada así como no tiene nada que perder. Este sistema proporciona un nivel mucho mas alto en seguridad y los parámetros que los contiene no pueden ser alterados.

Para el objeto de este trabajo, el uso de un sistema biométrico en el proceso de identificación de personal, busca solucionar el problema de reconocimiento, determinando la identidad de una persona y la verificación que busca confirmar o denegar la identidad que aduce una persona."Una verificación

certera de la identidad de una persona podría disuadir la delincuencia y el fraude, dinamizar las transacciones comerciales y salvaguardar los recursos críticos". (Travieso, 2011. p.8)

Un sistema biométrico hace referencia a una tecnología de punta, la cual consta de una serie de componentes los cuales son fundamentales para comprender el funcionamiento de los sistemas biométricos:

1. Sensor: dispositivo que captura los rasgos o características biométricas. De acuerdo a los rasgos que se requieran registrar o el tipo de tecnología biométrica, se necesitan diferentes tipos de sensores entre los cuales se encuentran:

Tabla 1. Tipos de sensores

Tecnología	Dispositivo de captura
Huella dactilar	Periférico de escritorio, tarjeta PCMCIA o lector integrado.
Reconocimiento de voz	Micrófono o teléfono
Reconocimiento facial	Cámara de video o cámara integrada
Reconocimiento de iris	Cámara de infrarrojos
Reconocimiento de retina	Unidad propietaria de escritorio o de pared
Reconocimiento de la geometría de la mano	Unidad propietaria de pared o de pie
Reconocimiento de a firma	Tableta de firma, puntero sensor al movimiento
Reconocimiento de escritura de teclado	Teclado

Fuente: Travieso (2008)

2. Repositorio: Es la base de datos donde se almacenan las plantillas biométricas inscritas para su comparación. Debería protegerse en un área física segura, así como ser cifrada y firmada digitalmente.
3. Algoritmos: Usados para la extracción de características (procesamiento) y su comparación. Las tres funciones básicas asociadas a ellos son: registro, verificación e identificación. (Pérez, 2011 p.24)

El registro en el sistema, es el registro de identidad que los usuarios hacen y se hace a través de la obtención de los parámetros biométricos. Este registro consta de tres fases distintas:

1. Captura: recolección de parámetros biométricos y depende de la tecnología biométrica así:

Tabla 2. Tecnología biométrica

Tecnología	Muestra biométrica
Huella dactilar	Imagen o minucia de la huella dactilar
Reconocimiento de voz	Grabación de voz
Reconocimiento facial	Imagen facial
Reconocimiento de iris	Imagen del iris
Reconocimiento de retina	Imagen de la retina
Reconocimiento de la geometría de la mano	Imagen en 3-D de la parte superior y lateral de mano y dedos
Reconocimiento de a firma	Imagen de la firma y registro de medidas relacionadas con la dinámica
Reconocimiento de escritura de teclado	Registro de las teclas pulsadas y registro de medidas relacionadas con la dinámica

Fuente: Pérez, 2011

2. Procesamiento: generación de la plantilla con las caracteristicas personales de los parametros capturados, los diferentes rasgos son:

Tabla 3. Rasgos de características capturadas

Tecnología	Muestra biométrica
Huella dactilar	Ubicación y dirección del final de las minucias o formas de las huellas
Reconocimiento de voz	Frecuencia, cadencia y duración del patrón vocal.
Reconocimiento facial	Posición relativa y forma de la nariz, posición de la mandíbula
Reconocimiento de iris	Surcos y estrías del iris
Reconocimiento de retina	Patrones de los vasos sanguíneos de la retina
Reconocimiento de la geometría de la mano	Altura y anchura de los huesos y las articulaciones de los dedos y de la mano
Reconocimiento de la firma	Velocidad, orden de los trazos, presión y apariencia de la firma
Reconocimiento de escritura de teclado	Secuencia de teclas y pausas entre pulsaciones

Fuente: Pérez, 2011

3. Inscripción: una vez completa la inscripción en la plantilla el sistema puede autenticar a las personas con el uso de esta plantilla. (Pérez, 2011 p.25)

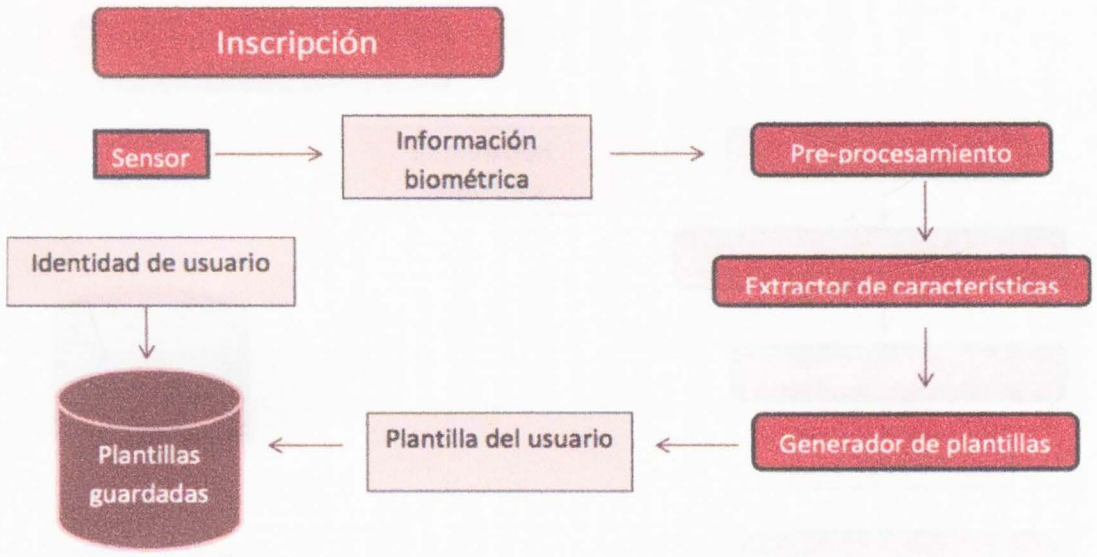

Figura 4. Proceso de inscripción en un registro biométrico

Fuente: Pérez, 2011

La autenticación es el proceso en el que se comparan las capturas de muestras biométricas con plantillas ya registradas y se dan de dos formas diferentes:

1. Identificación: compara la muestra recogida de un usuario frente a una base de datos biométricos registrados previamente. "No se precisa de declaración inicial de su identidad por parte del usuario, es decir, el único dato que se utiliza es la muestra biométrica recogida en el momento de uso, sin apoyo de un registro anterior ni un nombre de usuario o cualquier otro tipo de reconocimiento". (Pérez, 2011 p.26)

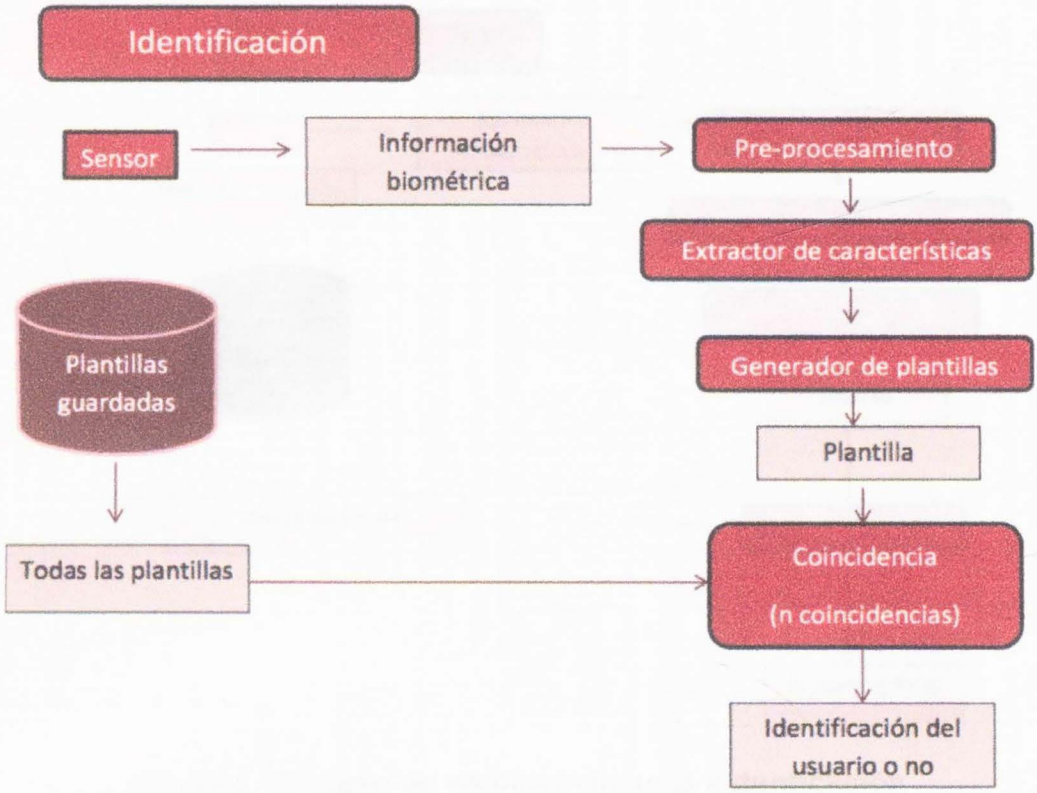

Figura 5. Proceso de identificación en la autenticación

Fuente: Pérez, 2011

2. Verificación: siendo el primer paso del proceso la identificación, se selecciona el patrón, el sistema recoge la característica biométrica y se compara con la almacenada y el resultado es positivo o negativo. (Pérez, 2011 p.27)

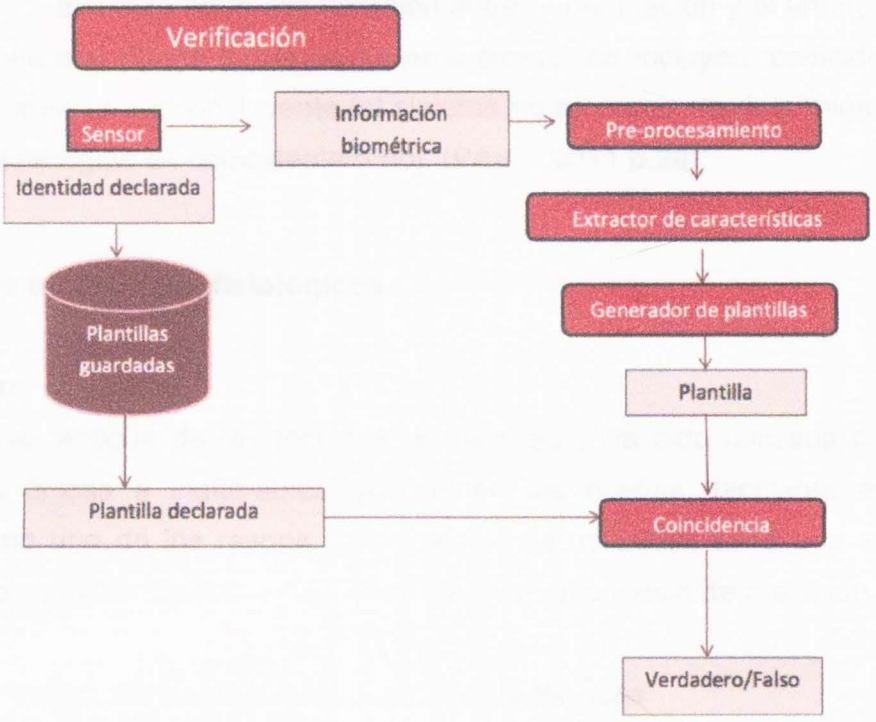

Figura 6. Proceso de verificación en la autenticación

Fuente: Pérez, 2011

Para la toma de decisiones, la biometría tiene 4 etapas:

1. Búsqueda de coincidencias: comparación de las muestras para determinar grado de similitud
2. Cálculo de una puntuación: valor numérico que indica el grado de similitud o correlación entre las muestras. Los sistemas biométricos se basan en algoritmos de búsqueda de coincidencias que generan una puntuación. Esta puntuación representa el grado de correlación entre la muestra a autenticar y la de registro.
3. Comparación con el umbral establecido: es un numero predefinido, que establece el grado de correlación necesario para que una muestra se considere similar a otra.

4. Decisión: Resultado de la comparación entre la puntuación y el umbral. Las decisiones que puede tomar un sistema biométrico incluyen: coincidencia, no coincidencia e inconcluyente (el sistema no es capaz de determinar si la muestra recogida es coincidente o no). (Pérez, 2011 p.28)

8.1.1 Sistemas biométricos fisiológicos

Huella Dactilar

Es la mas antigua de las técnicas biométricas y ha sido utilizada por las características únicas e inalterables que tienen las huellas dactilares en las personas. Como uno de los rasgos biométricos más utilizados tiene una amplia gama de tecnologías de captura y funciones; tiene un alto indice de precisión.

Dentro de las huellas dactilares existen dos tipos de técnicas:

1. Basada en minucias: formas fácilmente identificables existentes en la huella. A partir del tipo de minucia y la posición en la huella se establecen las mediciones y se crea el modelo o plantilla para cada usuario.
2. Basada en correlación: se analiza un patrón global seguido de la huella dactilar, esta técnica requiere de un registro preciso.

Reconocimiento facial

Es el reconocimiento de una persona a través de una imagen o fotografía, en esta técnica se utilizan programas de cálculo que analizan imágenes de rostros humanos. Dentro de los aspectos mas utilizados para la comparación está la distancia entre los ojos, la longitud de la nariz o el Angulo de la mandíbula. (Pérez, 2011).Este sistema es utilizado para la vigilancia general mediante cámaras de video.

Reconocimiento del iris

El iris humano tiene patrones que vienen desde el nacimiento y rara vez cambian ya que tienen gran cantidad de información y mas de 200 propiedades únicas. Este sistema se lleva a cabo mediante una cámara de infrarrojos el cual toma una foto en alta resolución los cuales se almacén para posteriormente realizar las verificaciones. Ante las diferencias y dificultad de captar los patrones entre el ojo izquierdo o derecho de las personas hace que este sistema sea uno de los más resistentes al fraude.

Reconocimiento de la geometría de la mano

Utiliza la forma de la mano y se toma a través de una cámara 3D en diferentes ángulos de la mano. Dentro de las características que se extraen están las curvas de los dedos, grosor, longitud, altura, anchura, distancias entre articulaciones y estructura ósea. Circunstancias como inflamaciones o lesiones pueden varia la estructura de la mano lo que afectaría la identificación.

Reconocimiento de retina

Se basa en los vasos sanguíneos contenidos en la retina. El hecho de que cada patrón sea único (incluso en gemelos idénticos al ser independiente de factores genéticos) y que se mantenga invariable a lo largo del tiempo, la convierten en una técnica idónea para entornos de alta seguridad. (Pérez, 2011).

8.1.2 Sistemas biométricos de comportamiento

Reconocimiento de firma

Analiza la firma manuscrita a través de dos variantes:

1. Comparación simple: grado de parecido entre dos firmas (original y la que se está verificando)
2. Verificación dinámica: análisis de la forma, velocidad, presión del boligrafo y duración del proceso de firma.

Reconocimiento de voz

Usan redes neuronales para aprender a identificar voces. Se hace a través de algoritmos que miden y estiman la similitud para devolver un resultado, la identificación se puede complicar por ruidos de fondo. Este sistema se usa para centro de atención a llamadas telefónicas que para controles de acceso.

Reconocimiento de escritura de teclado

Se basa en el hecho de un patrón de escritura en teclado propio de cada individuo, midiendo asi la fuerza del tecleo, duraciones, pulsaciones y tiempo entre presión de las teclas.

Reconocimiento de la forma de andar

Referencia la forma de andar de una persona la cual es grabada y se somete a un proceso analítico generando una plantilla biométrica derivada del comportamiento. Esta tecnología esta en desarrollo.

8.1.3 Criterios para definir un sistema biométrico

Para definir que tipo de tecnología biométrica se debe utilizar, deben evaluarse los siguientes parámetros: grado de aceptación, resistencia al fraude, mensurabilidad, comportamiento, permanencia, unicidad, universalidad.

Entre los estudios que se han hecho a los diferentes tipos de tecnologías encontramos la siguiente información:

	Grado de Aceptación	Resistencia al fraude	Mensurabilidad	Comportamiento	Permanencia	Unicidad	Universalidad
Huella dactilar	M	A	M	A	A	A	M
Reconocimiento facial	A	B	A	B	M	B	A
Reconocimiento de iris	B	A	M	A	A	A	A
Geometría de la mano	M	M	A	M	M	M	M
Reconocimiento de retina	B	A	B	A	A	A	A
Geometría de venas	M	A	M	M	M	M	M
Reconocimiento de voz	A	B	M	B	B	B	M
Reconocimiento de firma	A	B	A	B	B	B	B
Reconocimiento de escritura de teclado	M	M	M	B	B	B	B
Forma de andar	A	M	A	B	B	B	M

A: Alto M: Medio B: Bajo

Figura 7: Valoración comparativa de las distintas técnicas biométricas

Fuente: Pérez, 2011

Tecnología	Ventajas	Inconvenientes
Huella dactilar	• Alto grado de madurez • Costes de implantación reducidos • Buena aceptación	• Incompatibilidad con determinados trabajos manuales
Reconocimiento de voz	• No requiere inversión en dispositivos • Posibilidad de autenticación remota	• El ruido de fondo dificulta la captura • Dificultad para reconocer ciertas formas de hablar
Reconocimiento facial	• Reconocimiento en multitudes • Identificación a media distancia • Buena aceptación	• Escasa resistencia al fraude • Unicidad limitada

Tecnología	Ventajas	Inconvenientes
Reconocimiento de iris	• Patrones muy complejos • Unicidad muy alta • Alto grado de permanencia	• Coste de implantación alto • Menor grado de aceptación
Reconocimiento de retina	• Unicidad muy alta • Alto grado de permanencia	• Precisa de total colaboración del usuario
Reconocimiento de la geometría de la mano	• Alto grado de permanencia • Facilidad de uso	• Unicidad limitada
Reconocimiento de firma	• Buena aceptación • Facilidad de uso	• Dificultad de captura por cambios de posición
Reconocimiento de escritura de teclado	• No requiere inversión en dispositivos • Posibilidad de realizar monitorización	• Tecnología emergente

Figura 8.Ventajas e inconvenientes de las distintas tecnologías

Fuente: Pérez, 2011

Dentro de las aplicaciones actuales de la biometría se encuentran el control de accesos físicos y lógicos; control de presencia; control de fronteras; lucha contra el fraude; investigación de delitos; y acceso a servicios y ayudas gubernamentales.

8.2. COMPATIBILIDAD O INCOMPATIBILIDAD DE LOS SISTEMAS DE SEGURIDAD EXISTENTES CON UN SISTEMA DE IDENTIFICACIÓN FACIAL BIOMÉTRICO

Dentro de las aplicaciones mas estudiadas en el campo de la biometría se encuentra la del reconocimiento facial automatizado. Esta forma de reconocimiento desarrollada desde los años 60, inicio de forma semiautomatizada y requería de un administrador para localizar rasgos especificos en las fotografías

(boca, las orejas, la nariz y los ojos) para después ser comparados con datos de referencia.

En los años 70 Goldstein, Harmon, & Lesk (1971), 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 & Sirobich aplicaron el análisis de componentes principales, 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 (Sirovich, 1987, p.519 - 524).

En 1991 Turk & Pentland utilizando las técnicas Eigenfaces, descubrieron que el error residual podía ser utilizado para detectar caras en las imágenes, lo que permitió llegar a los sistemas automatizados de reconocimiento facial en tiempo real y autentico. (p.586-591)

Esta tecnología ha llamado la atención del público, una de las primeras implementaciones fue la del Súper Bowl de la NFL en enero de 2001, que capturó imágenes de vigilancia, las cuales fueron comparadas con una base de datos de foto archivos digitales. Esto demostró como usar la tecnología para satisfacer necesidades nacionales, pero causó grandes reacciones en el tema de la 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. (Métodos biométricos: reconocimiento facial)

Existen dos familias de técnicas de reconocimiento facial: técnicas basadas en la apariencia y técnicas basadas en modelos en cada una de estas se encuentran varios métodos para caracterizar la imagen (Xiaoguang Lu, 2003).

Los sistemas basados en la apariencia se utilizan directamente sobre las imágenes sin hacer uso de modelos 3D. Estos tipos de sistemas representan un objeto en función de diferentes vistas del mismo. En estos sistemas cada imagen se representa como un punto en un subespecio vectorial, de forma que la comparación entre la imagen de test y las imágenes de referencia se realiza en el subespacio vectorial caras. El objetivo de estos algoritmos es clasificar las diferentes caras en el nuevo subespacio, pero para ello será necesario entrenar previamente el sistema con imágenes de diferentes caras con diferentes vistas. (Hernandez, 2010, p.15)

Los sistemas basados en modelos, intentan construir un modelo lo más descriptivo posible de la cara humana capaz de detectar con precisión las variaciones faciales. Estos sistemas tratan de obtener características biométricas de las imágenes para realizar el reconocimiento (distancia entre ojos, grosor de la nariz...). Habitualmente estas técnicas requieren de imágenes de gran resolución. Cuando se utilizan estos sistemas, el algoritmo sabe con antelación el objeto que ha de representar y lo que intenta hacer es que corresponda la cara real con el modelo. (Hernández, 2010, p.16)

Cuando se usan las técnicas anteriormente mencionadas el proceso de construcción del sistema biométrico consta de tres pasos:

- Construcción del modelo.
- Ajustar el modelo a la imagen de test.
- Utilizar los parámetros del modelo ajustado para calcular la similitud
- Entre la imagen de test y las imágenes de referencia para realizar el reconocimiento. (Xiaoguang Lu, 2003)

8.2.1 Reconocimiento de imágenes fijas

Requiere de un reconocimiento a través de los siguientes bloques:

Figura 9. Reconocimiento de imágenes fijas

Fuente: Hernández, 2010

En este sistema hace uso de los siguientes conjuntos de imágenes

> Imágenes de referencia: son las que están almacenadas y son conocidas por el sistema y son utilizadas para saber si una imagen de entrada pertenece o no a algún sujeto registrado en el sistema.
>
> Imágenes de test: son las que recibiremos en el sistema y se tienen que reconocer.
>
> Imágenes de entrenamiento: son utilizadas en los métodos PCA y LPP para conseguir las matrices de proyección. (Hernández, 2010, p.18)

El proceso de este reconocimiento es el siguiente: (no tiene en cuenta el pre procesado previo de las imágenes)

1. El sistema necesita de un set de imágenes de referencia las cuales son procesadas y proyectadas en el nuevo subespacio para después ser utilizadas para conocer si una imagen pertenece o no a un individuo registrado en el sistema
2. Cuando las imágenes de referencia están correctamente proyectadas, se realiza el mismo procedimiento con las imágenes de test. Estas pueden pertenecer a personas que estaban incluidas entre las imágenes de referencia pero mostrando diferentes expresiones faciales o diferentes condiciones del entorno.
3. Finalmente se dirá que ha habido reconocimiento si se cumple alguna condición, en general se considera que hay un reconocimiento positivo si se cumple una condición. (Hernández, 2010, p.19)

8.2.2Principales técnicas

8.2.2.1 *PCA (Principal ComponentAnalysis)*: método que transforma un número de variables que permite encontrar los vectores que mejor representan la distribución de un grupo de imágenes. PCA permite representar una imagen de una cara usando una base que se ha conseguido a partir de muchas observaciones de diferentes caras. "El objetivo de este método consiste en representar una imagen en términos de un sistema de coordenadas óptimo reduciendo el número final de componentes que tendrá la imagen" (Hernandez, 2010, p.20)

8.2.2.2 *LDA(Linear Discriminant Analysis)*: tiene como objetivo convertir un problema de alta dimensionalidad en uno de baja. En este sistema se proyectan las imágenes en un espacio vectorial de baja dimensionalidad de manera que la ratio entre la distancia entre clases y la distancia dentro de la

clase se maximiza. De este modo se garantiza una máxima discriminación entre las clases. (Hernández, 2010, p.22)

8.2.2.3 *LPP (Locality preserving projections)*: es un algoritmo lineal que al igual que el PCA realiza una reducción dimensional de los datos. Es rápido y útil para aplicaciones prácticas. Este método conserva una estructura local de los datos lo que permite que las imágenes pertenecientes a un mismo individuo esten cercanas entre si y alejadas de las de otros individuos, lo que indica que hay una discriminación entre clases. (Hernández, 2010, p.24)

8.2.2.4 *DCT (Discrete Cosine Transform)*: es una transformación que representa una secuencia finita de datos, esta técnica es muy utilizada en aplicaciones de procesado de señal, desde compresión de audio e imágenes hasta métodos espectrales para la solución numérica de ecuaciones diferenciales. Una de estas aplicaciones es el reconocimiento facial. "A diferencia de PCA este método no necesita ser entrenado con imágenes del mismo tipo a las que se van a usar sino que simplemente se transforman directamente las imágenes, es decir, la base de la transformación es independiente de las imágenes". (Hernández, 2010, p.27)

8.2.2.5 *DCT por Bloques*: mezcla de las técnicas basadas en la apariencia y las basadas en modelos, en concreto, hace uso de la misma metodología que el método DCT pero aplicado de forma distinta. (Hernández, 2010, p.28)

8.2.3Métodos usados por los proveedores de reconocimiento facial

8.2.3.1 *Eigenface*: tecnología que utiliza imágenes bidimensionales en escala de grises que representan características distintivas de una imagen facial.

8.2.3.2 *Análisis de características locales*: mas utilizada en el reconocimiento facial, se adapta mejor a los cambios en la apariencia o aspecto facial. Hace un análisis de características locales utilizando

docenas de características de las diferentes de la cara e incorpora la ubicación relativa de los rasgos. Los datos arrojados son bloques de construcción que se utilizan para identificar o verificar.

8.2.3.3 *Neural Network Mapping*: las redes neuronales emplean un algoritmo para determinar la similitud de las características únicas de la muestra adquirida y de la obtenida en el registro, utilizando tantas partes de la imagen facial como sea posible.

8.2.3.4 *Procesamiento automático de la cara*: utiliza las ratios de distancia entre las características de fácil adquisición, tales como los ojos, la punta de la nariz y las comisuras de la boca. (Pérez, 2011).

Características de un sistema de reconocimiento facial:

- Sistema no invasivo (no intrusión física o contacto del autentificador con el sistema de reconocimiento).
- Permite la identificación de personas en movimiento.
- Sistema con posibilidad de camuflaje (las personas no detectan que son objeto de un proceso de reconocimiento).
- Reconocimiento de sujetos no dispuestos a cooperar.
- El sistema de captura necesita de una fuente de luz auxiliar.
- Susceptible a problemas de iluminación.
- Sistema vulnerable al reconocimiento de sujetos que se han sometido a operaciones de cirugía plástica (estéticas y de cirugía en general). (Espinosa, n.d)

Actualmente, las unidades del Ejército Nacional no cuentan con un sistema estandarizado de control de acceso a las unidades, el único sistema de identificación, está a través de los ficheros o documentos de identificación que portan las personas. El sistemas más avanzado es el que se encuentra en el Ministerio de Defensa para acceder a las oficinas de los comandos, en donde se hace a tráves de tarjetas autorizadas por un sistema de cómputo.

Al comparar este sistema con un sistema de tecnología biométrico se puede identificar que el sistema tradicional de identificación a través de tarjetas resulta vulnerable para la institución, estas pueden ser olvidadas, robadas e incluso están al alcance de terceros.

Los sistemas biométricos por su parte, garantizan una facilidad para los usuarios ya que estos no dependerán ni de tarjetas o acceso especiales para ser identificados, el sistema es altamente seguro y su vulnerabilidad tanto para un espionaje o como para un ataque por fuerza bruta es nula. Aunque los costos de implantación de un sistema biométrico facial son más costosos, a futuro los costos de mantenimiento son mucho menores a los sistemas de tarjetas o contraseñas ya que estos generan gastos asociados con la pérdida y olvido de estas.

La mayoría de los usos y aplicaciones de tecnologías biométricas se dan en el sector público y algunas destinados a la Defensa y Seguridad Nacional; "destacan sistemas para la identificación de terroristas y criminales, investigación forense, documentos nacionales de identidad, control fronterizo, control de acceso, control de presencia y gestión de ayudas públicas". (Pérez, 2011, p.55).

8.3 TIPO DE INFORMACIÓN Y RECURSOS NECESARIOS PARA ADOPTAR UN SISTEMA DE IDENTIFICACIÓN BIOMÉTRICO.

Para adoptar un sistema de identificación facial biométrico, se requiere que la alimentación de éste sea con los datos reportado por cada integrante de la fuerza, en la sección de hojas de vida de la Jefatura de Personal del Ejército, específicamente el literal "i". Del extracto de la hoja de vida(datos de identificación) se tomarían los siguientes datos: grado, especialidad, documento de identidad, código militar, apellidos y nombres completos, arma, especialidad, fecha y lugar de nacimiento, edad, estado civil, dirección de residencia, teléfono, unidad actual,

cargo actual, fecha de ingreso, tiempo de servicio, y por ultimo estado del empleado; además de la fotografía que serviría de patrón de comparación.

El sistema funcionaria como un "espejo", es decir el software o sistema de identificación facial biométrico, toma la imagen de la persona en la guardia, la cual será comparada con la de la base de datos (información del sistema actual de la Jefatura de Personal del Ejército), para identificar y verificar si pertenece o no al Ejercito y evitar la suplantación; esta información mostrará la imagen de la persona y la información relacionada del extracto de la hoja de vida en el literal "i".

Las personas que no estén incluidas en la base de datos del Ejército se irán almacenando en el software con la información básica registrada en la cédula, para identificar plenamente su identidad.

Beneficios de implementar un sistema de identificación facial biométrico:
Adicional a las bases matriz que tiene el Ejército Nacional para identificación del personal que labora en la institución, la implementación de un software para reconocimiento facial permitiría almacenar diferentes bases de datos con su respectiva información como son:

Registraduría: identificar plenamente la real identidad de una persona al pasar por la cámara.

Adicional a esto para el área de inteligencia militar el sistema permite que mediante una fotografía tomada durante una vigilancia o seguimiento, esta sea enviada y cotejada con las bases de datos previamente almacenadas en el software (especialmente la de la Registraduría) y en cuestión de minutos se tenga identificada plenamente la persona objeto de la vigilancia, es decir: por Registraduría estaría identificado plenamente, por fiscalía sabríamos su situación jurídica, y la demás información dependería de la cantidad de bases de datos que se encuentren almacenadas.

Fiscalía: permite conocerlos antecedentes judiciales de la persona que se encuentra en el campo visual de identificación de la cámara.

Transito y transporte: permite saber la información registrada en esta entidad.

Integrantes de organizaciones al margen de la ley (FARC, ELN, BACRIM: con la alimentación del software de fotos e información de integrantes de las OAML (ordenes de batalla), se permitirá identificar si la persona bajo el campo de la cámara pertenece a una de estas organizaciones al margen de la ley.

Se pueden citar dos casos de éxito de implementación de sistemas biométricos de tecnología facial, aplicados a la seguridad a nivel internacional, uno utilizado en las fronteras aeroportuarias en España y el segundo de gestión de ayudas públicas en Polonia.

Fronteras Aeroportuarias en España

Proyecto de implantación del sistema Automatic Border Crossing (ABC) para el acceso rápido a fronteras aeroportuarias por parte de Indra Systems, impulsado por el Ministerio del Interior del Gobierno de España a través de la Secretaría de Estado de Seguridad con destino la Comisaría General de Extranjería y Fronteras.

El objetivo del proyecto es la implantación de un sistema que automatice el paso fronterizo, en la medida de lo posible, de manera desatendida. Está destinado a viajeros cuyo origen o destino está fuera del ámbito europeo.

El sistema está formado por un conjunto de quioscos en los que se introduce un pasajero que verifica su identidad por medio del reconocimiento facial y de huella dactilar. Posteriormente, y ya verificada su identidad, accede a través de unas puertas automáticas. Adicionalmente, los agentes fronterizos están situados en una cabina próxima, desde la que

monitorizan todo el proceso e intervienen en caso de que lo consideren necesario.

El proceso comienza verificando físicamente el pasaporte mediante reconocimiento de patrones visuales y continúa verificando electrónicamente el chip que contiene este documento. Posteriormente lleva a cabo el reconocimiento dactilar y facial para acabar con una consulta a bases de datos policiales en busca de antecedentes o documentos robados.

Existen dos tipos de instalaciones: de puerta simple (quioscos distribuidos por la sala de la terminal y puertas de acceso automáticas) y de esclusa (quioscos integrados en las puertas automáticas; en estos si la verificación no tiene éxito el pasajero no puede avanzar).

El sistema es utilizado por 350 pasajeros diariamente, teniendo en cuenta que su uso no es obligatorio. El empleo de este sistema equivale al trabajo de ocho funcionarios policiales.

El proyecto ABC System. Control Automático de Fronteras desarrollado por el Ministerio del Interior ha sido galardonado con numerosos premios, entre otros el "Premio ENISE2 2010 al mejor servicio o proyecto con DNIe". (Pérez, 2011 p.63)

Gestión de ayudas públicas en Polonia:

Se trata de un proyecto de gestión de ayudas públicas otorgadas por el Gobierno de Polonia a través de cajeros automáticos, autenticando a los ciudadanos mediante el reconocimiento de la estructura de las venas de los dedos y un PIN.

Mensualmente un total de 2.000 personas hacen uso de la tecnología en cada una de las 65 sucursales en la que está instalada.

El objetivo es la gestión de las ayudas gubernamentales de forma segura, cómoda y automatizada. En un principio solamente se consideró la gestión de las prestaciones por desempleo pero actualmente su uso se ha ampliado a otras ayudas.

Con el uso de esta tecnología se pretende mejorar la eficiencia de la gestión de las ayudas gubernamentales. Hoy en día, si no se usa el sistema biométrico, la persona entrega un documento de identificación, el cual se comprueba, y se rellenan una serie de formularios. Este proceso se demora considerablemente en el tiempo. Esto suele conllevar la creación de largas colas de espera para poder acceder a las ayudas, provocando el descontento de los ciudadanos.

Sin embargo, utilizando el sistema implantado, el usuario puede acudir a un cajero automático a la hora que le resulte más conveniente para obtener la ayuda. Esta comodidad es beneficiosa tanto para el banco, aliviando sus oficinas de clientes pudiendo ofrecer un mejor servicio, como para el usuario, que no necesita acudir en horario de apertura de oficinas. (Pérez, 2011 p. 66)

9. CONCLUSIONES Y RECOMENDACIONES

Uno de los principales beneficios del sistema de identificación biométrico, es que durante su implementación nos garantizaría que la persona que pretende ingresar a una guarnición militar es quien dice ser y demuestra ser mediante algún documento es que garantizan que la persona es quien dice ser, es decir, que el sistema compararía los rasgos de la persona que intenta acceder a la unidad con los depositados en la base de datos y este arrojaría la información del funcionario a quien pertenece.

A través de la implementación de este sistema se eliminaría el riesgo de robos o falsificación de tarjetas de identificación, las cuales facilitan los accesos por las guardias, lo cual anularía este antiguo proceso de identificación y sometería a las personas a ser objetos del escaneo facial por parte del sistema y es este quien informe si la persona que intenta acceder a la guardia es realmente quien dice ser.

Con la implementación de este sistema se reducirían los costos generados por la fabricación de ficheros, así mismo la reducción del tiempo empleado al trámite de ficheros de los funcionarios que laboren en la oficina de seguridad.

La adopción del sistema de identificación facial biométrico aumentaría considerablemente la eficiencia en materia de seguridad, respecto al proceso de identificación de las personas, reduciendo ostensiblemente los márgenes de vulnerabilidad frente a las suplantaciones de las que constantemente son objeto las diferentes guardias del Ejército Nacional. Un sistema biométrico facial genera un aumento en el índice de eficiencia, ya que hace que los procesos de ingreso a las unidades sean en corto tiempo agilizando así los procesos que tienen los comandantes de guardia a la hora de la verificación del personal que ingresa a las unidades.

El sistema biométrico facial es un elemento esencial en la búsqueda del mejoramiento continuo de la seguridad física y de personas, que garantizaría cumplir con estándares óptimos de calidad en la prestación de servicios de seguridad integral, alineándose con el éxito y desarrollo de los objetivos trazados por la institución

La implementación de un sistema biométrico facial para el Ejercito Nacional, permitiría estar a la vanguardia tecnológica a nivel mundial, coadyuvando a identificar y contrarrestar nuevas amenazas dentro de los retos del futuro.

RECOMENDACIONES

Tomar contacto con empresas que fabriquen este sistema de identificación facial biométrico, para conocer de primera mano las bondades que ofrece este sistema, identificar características técnicas, funcionabilidad y su aplicabilidad para la fuerza y porque no, otras fuerzas

Con el apoyo de empresas que provean este sistema, realizar pruebas de campo tomando como modelo algunas guardias de unidades del Ejército que permitan evidenciar la aplicabilidad para neutralizar los casos de suplantación que se puedan presentar en un futuro.

Adoptar este sistema en las guardias del Ejército y alimentar la base de datos con información de la Registraduría Nacional, para conocer realmente la identidad de la persona, además contando con la base de datos de la Fiscalía General de la Nación, se podría conocer inmediatamente si la persona que sea objeto del escaneo del sistema tiene antecedentes penales (solo las personas que tengan almacenada la fotografía en la base de datos de la fiscalía).

10. REFERENCIAS

Ejército Nacional (2009). *Manual de Seguridad Milita* (2ª. Ed.). Bogotá, Colombia.

Ejército Nacional (2009). *Resolución Número 1692: "Reglamento de régimen interno para unidades tácticas"*. Bogotá: Fuerzas Militares de Colombia.

Escuela Superior de Guerra (2013) *Guía Metodológica de Investigación*. Bogotá, Colombia: ESDEGUE-SIIA-CEESEDEN

Espinosa, V. (n.d) *Evaluación de Sistemas de Reconocimiento Biométrico*. Barcelona, España: Escuela Universitaria Politécnica de Mataró.

Eyssautier, M. (2006) *Metodología de la investigación*. México: Thomson Editores.

Goldstein, A. J. Harmon, L. D. y Lesk, A. B. (1971*) Identification of Human Faces*. Proc. IEEE. Vol. 59, No. 5. Extraído el 19 de junio de 2013 desde http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Hernández, R.G. (2010) *Estudio de técnicas de reconocimiento facial*. Barcelona, España: Universidad Politécnica de Cataluña.

Martín G., C. (2009) *El documento y sus clases. Análisis documental: indización y resumen*. Extraído el 24 de junio de 2013 desde http://eprints.rclis.org/14605/1/tipdoc.pdf

Métodos biométricos: reconocimiento facial. (n.d.). Extraído el 19 de junio de 2013 desde http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Pérez, P., Álvarez, E., De la Fuente, S., y García, L. (2011). *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*. Madrid, España: Instituto Nacional de Tecnologías de la Comunicación (INTECO)

Pérez, P., Álvarez, E., De la Fuente, S., y García, L. (2011). *Guía sobre las tecnologías biométricas aplicadas a la seguridad*. Madrid, España: Instituto Nacional de Tecnologías de la Comunicación (INTECO)

Pérez C, J.C., y Paredes, R. (n.d) *Sistemas de seguridad basados en características biométricas*. Extraído el 24 de Marzo de 2013 desde http://www.iti.es/media/about/docs/tic/07/2005-06-biometria.pdf

Presidencia de la República (1991). *Constitución Política de Colombia*.

Pruebas piloto de reconocimiento facial en cajeros (n.d). Extraído el 24 de Marzo de 2013 desde http://biometria.smartmatic.com/category/reconocimiento-facial

Sánchez, C.A. (n.d.). *La experiencia colombiana en identificación biométrica aplicada a las elecciones*. Extraído el 24 de Marzo de 2013 desde http://www.registraduria.gov.co/-Biometria-.html

Sirovich, L. y Kirby, M. (1987) *A Low-Dimensional Procedure for the Characterization of Human Faces*. J. Optical Soc. Am. A. Vol. 4, No.3. Extraído el 19 de junio desde http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Técnicas de la investigación (n.d). Extraído el 13 de junio de 2013 desde http://www.universitas.net.ve/biblioteca/datados/documental.pdf

Travieso, C.M., del Pozo, M. Y Ticay, J.R (2011). *Sistemas Biométricos*. Las Palmas, España: Universidad de las Palmas de Gran Canaria.

Turk, M.A. y Pentland, A. P. (1991) *Face Recognition Using Eigenfaces*. Proc. IEEE. Extraído el 19 de junio de 2013 desde http://www.biometria.gov.ar/metodos-biometricos/facial.aspx

Ventajas de la autenticación biométrica (n.d). Extraído el 24 de Marzo de 2013 desde http://biometria.smartmatic.com/ventajas-de-la-autenticacion-biometrica

Xiaoguang L. (2003) *"Image analisis for FACE Recognition"*, Department of Computer Science & Engineering, Michigan State University.