Panorama de la biometría de huellas dactilares en Colombia

Medina Gutiérrez Ángela María, Castelblanco Peñuela Andrés Camilo
Universidad Piloto de Colombia, Especialización en Seguridad Informática,
Bogotá, Colombia
ing_angela_medina@hotmail.com
accp08@gmail.com

Resumen-- *El propósito del presente artículo es realizar una perspectiva de las huellas dactilares en dispositivos biométricos, en donde se evaluará desde el punto de vista de la seguridad informática el uso de esta tecnología, como mecanismo de identificación y autenticación de personas en el sector público y privado en Colombia*

De esta manera, se pretende generar un panorama del empleo de estas tecnologías, que ayude a los directivos de los diferentes sectores, a tomar decisiones de la implementación o no de las mismas en sus organizaciones.

Abstract – The purpose of this article is to provide a perspective of fingerprint biometric devices, where will be assessed since the point of view of information security the use of this technology, as a means of identification and authentication of people, in the public and private sectors in Colombia.

In this way, it aims to create an overview of the use of these technologies to help managers in different sectors, to make decisions about or not implementing them in their organizations.

Índice de términos-- *Biometría, dactilograma, forense, hacking.*

Terms Index -- Biometric, dactylogram, forensic, hacking.

I. INTRODUCCIÓN

El mundo da pasos agigantados en seguridad y tecnología; siendo este un factor clave para la protección de datos personales. Colombia sin embargo se prepara para reglamentar el uso y protección de las libertades y derechos fundamentales de las personas, en sistemas de información, bases de datos y dispositivos electrónicos de autenticación que son utilizados en entidades públicas y privadas.

Sin lugar a duda las herramientas tecnológicas y el uso indebido de datos personales han llevado a presentar una legislación que busca proteger la identidad de las personas, así como también fortalecer los mecanismos utilizados a través de biométricos para los diferentes trámites, servicios y transacciones en línea.

Colombia a través del tiempo ha visto la necesidad de automatizar procesos y de hacerlos eficientes, de conectar sus industrias y productos a través de mercados electrónicos, cuyo fin es generar impactos positivos tanto en las organizaciones como en sus usuarios a nivel local, regional, nacional o internacional con la apropiación de tecnologías de la información.

Este pilar requiere que las entidades del sector privado y público tomen conciencia e inviertan recursos en la protección de datos, por ende para garantizar estos procedimientos son necesarios los mecanismos de autenticación, que validen que las personas involucradas en los procesos son quienes dicen ser, a partir de conductas o características propias del ser humano.

II. PRINCIPIOS DE LA BIOMETRÍA

En la antigüedad se estudiaba la forma de detectar un patrón que permitiera identificar a los seres humanos de los demás, pero de una manera única e inequívoca. Teniendo en cuenta lo anterior, la primera aplicación de una característica biométrica para la identificación, data en el siglo VIII en China, el cual consistía en aplicar huellas dactilares a los papiros y figuras de arcilla.

Posteriormente Quintiliano en el siglo X, empleó una marca de palmas salpicadas de sangre para resolver un delito y luego Marcelo Malpigio en 1686, realizó la primera investigación sistemática de huellas dactilares.

Seguidamente en la historia el profesor Jan Evangelist Purkinje clasifica en su tesis 9 formas de huellas dactilares; luego Sir William Herschel valida los contratos de la huella del pulgar como método de identificación de personas analfabetas; posteriormente el dirigente de delitos criminales de París Alphonse Bertillon, utilizó las cualidades del cuerpo para reconocer delincuentes a través de la fotografía métrica.

Después Henry Faulds, realizó estudios sobre las huellas estampadas en las cerámicas antiguas y propuso un método para clasificarlas al igual que también fue quien propuso las huellas dactilares a través de tintas.

Fue entonces cuando el croata Juan Vucettich logró instaurar que las huellas dactilares distinguían a una persona de otra, las cuales se fueron almacenando para permitir su cotejamiento y de esta manera poder recolectarlas en una escena del crimen [0].

III. BIOMETRÍA

El término biometría viene del griego "bios" que significa de vida y "metron" de medida. Como su nombre lo indica es un mecanismo que proporciona variables únicas con las que se puede reconocer una persona, a través de su fisiología o comportamientos.

Las características de atributos fisiológicos son consistentes, puesto que no cambian en el tiempo, salvo que sean alteradas por alguna enfermedad, trabajo o accidente el cual varíe la morfología de estas propiedades en las personas, mientras que el comportamiento tiene un margen de menos consistencia, porque dependen directamente de la naturaleza o personalidad humana.

Dichas características para convertirse en indicadores, deben cumplir con unas propiedades para poder ser utilizadas en procesos biométricos. Estas son:

A. *Universalidad.* Toda persona tiene esta característica.

B. *Distintividad.* La probabilidad de encontrar a 2 personas con una propiedad igual es baja.

C. *Estabilidad.* El patrón o característica permanece invariable en un periodo o tiempo razonable.

D. *Evaluabilidad.* La característica puede ser evaluada o medida en forma cuantitativa.[1]

Estas propiedades han ayudado a que los sistemas de seguridad se transformen, en la búsqueda de nuevas técnicas fiables, que puedan ser implementadas en los sistemas biométricos.

Por consiguiente se entiende por sistema biométrico, como un método automatizado que identifica y verifica a una persona a través de sus características físicas o comportamientos. Hoy en día la biometría se usa en organizaciones privadas y/o públicas porque ofrece un margen de seguridad medianamente alto, ya que son confiables y porque han demostrado su fidelidad en la autenticación y control de acceso de individuos.

Otra de las razones del uso de biométricos, es porque no requieren de entrenamiento para su utilización, son cómodos para los usuarios y de fácil manejo.

Un sistema biométrico tiene que considerar 3 características básicas, para la identificación personal las cuales se mencionan a continuación:

A. *El Desempeño.* Es la precisión, velocidad y robustez aceptable de un sistema biométrico en la identificación de personas.

B. *La Aceptabilidad.* Es el grado de disposición que tienen las personas para aceptar un biométrico en su ambiente diario.

C. *La Fiabilidad.* Evidencia el grado de dificultad para violar al sistema, esta se basa principalmente en reconocer patrones de una persona. [2]

Cabe resaltar que un sistema biométrico utiliza una arquitectura de dos módulos, los cuales explican claramente la funcionalidad de este proceso.

- *Módulo 1 Inscripción.* Este proceso adquiere el atributo del usuario por el lector biométrico, lo convierte en formato digital y luego lo procesa en el extractor de características, con el fin de emitir una imagen compacta que será almacenada en una base de datos.

- *Módulo 2 Identificación.* Este proceso se encarga del reconocimiento de personas, puesto que coteja los atributos del individuo, con uno o más patrones almacenados en la base de datos, para establecer la identidad del mismo. [3], [4].

Finalmente los biométricos se han posicionado como una clara alternativa de seguridad a seguir, porque protegen redes, información y demás activos críticos de una entidad.

IV. CLASES DE BIOMETRÍA

Existen muchas tecnologías en la actualidad que son utilizadas por biométricos, como lo muestra la Fig.1

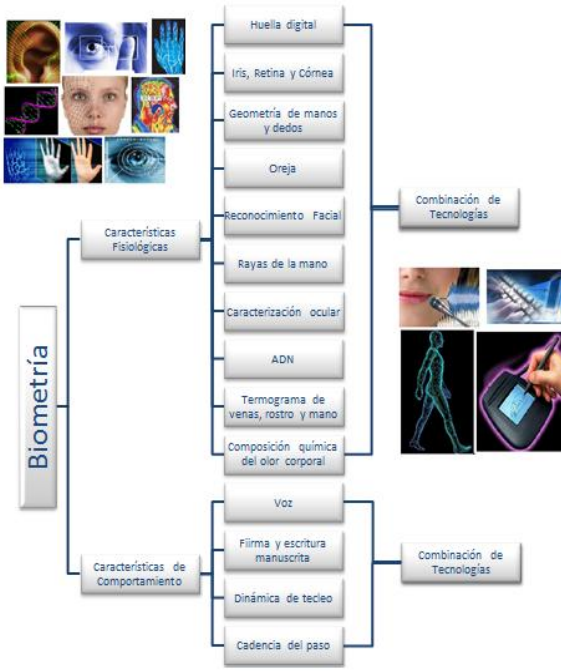

Fig. 1 Clasificación de biométricos.

Cada clase tiene debilidades y fortalezas, y su selección depende del costo, del nivel de seguridad y de la necesidad que se tenga. Sin embargo las huellas dactilares son las más empleadas ya que es el biométrico mas maduro del mercado, tienen una gran facilidad de uso y no son tan invasivas; dadas estas propiedades este artículo se centra en este tipo de biometría.

V. HUELLA DACTILAR

El antropólogo Juan Vucettich fue el primero en poner en práctica un sistema de identificación de personas por huellas dactilares, los primeros análisis se realizaron para esclarecer un crimen en argentina, cuando se dieron cuenta de lo óptimo y eficiente que era el método para establecer la identidad de un individuo, la policía de Buenos Aires adoptó el método para cotejamiento de las huellas dactilares de los reclusos en las cárceles de la ciudad; con el tiempo se convirtió en una ciencia llamada dactiloscopia.

Los patrones únicos de las huellas dactilares como la perennidad, la inmutabilidad y la diversidad infinita, garantizan que la huella desde la formación del feto hasta la muerte del individuo permanezcan sin cambios y sean únicas e irrepetibles; cuando se quiere cotejar una huella se usa los dactilogramas los cuales son los dibujos o figuras formadas por una huella sobre una superficie; los dactilogramas se pueden clasificar en tres tipos:

- *"Dactilograma natural. Es el que está en la yema del dedo, formado por las crestas papilares de forma natural.*

- *Dactilograma artificial. Es el dibujo que aparece como resultado al entintar un dactilograma natural e imprimirlo en una zona idónea.*

- *Dactilograma latente. Es la huella dejada por cualquier dactilograma natural al tocar un objeto o superficie. Este dactilograma queda marcado, pero es invisible. Para su revelación requiere la aplicación de un reactivo adecuado."* [5]

Con el avance de la tecnología el proceso de toma de huellas dactilares se ha ido automatizando para su cotejamiento; la primera forma de llevar la huella a un computador fue realizando un escaneo de la misma en papel, este proceso aunque un poco lento llevaba las huellas a una máquina para ser cotejadas. Sin embargo después de unos años se crearon dispositivos llamados huelleros electrónicos, los cuales de una forma automática pasan la imagen de la huella directamente al computador, haciendo el proceso mucho más rápido y efectivo.

El proceso biométrico de huella dactilar, es el más popular puesto que es de fácil acceso, tiene una aceptabilidad superior al 96%, tiene una probabilidad de huellas iguales de 1 a 64 mil millones y tiene un sistema de backup de 10 "hasta de los 10 dedos de la mano" [6] sin embargo también posee sus contras asociados a enfermedades y posibles accidentes que tenga durante la vida el individuo.

VI. BIOMETRÍA DE HUELLA DACTILAR PARA EL SECTOR PÚBLICO

Las entidades de carácter oficial o público se han centrado principalmente en la aplicación de mecanismos, que permitan establecer la identidad de las personas y que a su vez les proporcione herramientas para desarrollar políticas, estrategias y proyectos de inclusión digital.

Sensibilizar a los actores participantes del sector público, ha sido uno de los grandes retos para poder bajar el índice de brecha digital en la población.

Actualmente en Colombia este proceso de identificación única de individuos a través de sus huellas dactilares, es llevada a cabo por la Registraduría Nacional del Estado Civil. Se ha detectado que uno de los delitos que más aqueja al país es el fraude electoral por suplantación, medida que llevó al estado a pesar en soluciones tecnológicas para ayudar a bajar el índice de frecuencia de este delito.

La base que dio como resultado la aplicación de este tipo de tecnología, "*fue el análisis de las sentencias de nulidad proferidas por el Consejo de Estado en los años 2005 y 2009, mediante las cuales se anularon las actas de escrutinio de las elecciones de Congreso 2002 y 2006"*. [7]

Como medio se implementó el uso de dispositivos biométricos de huella dactilar para darle solución a este problema; la primera vez que se utilizó este mecanismo de identificación fue el 22 de Febrero de 2009 en una elección atípica de Alcalde Municipal en Belén de los Andaquíes, departamento de Caquetá, siendo un éxito, por lo que este método se ha estado utilizando en otras elecciones atípicas de comicios; a la fecha se han realizado 33 elecciones de este tipo, la última de ellas se celebró el 23 de Septiembre de 2012, para elegir Alcalde en el municipio de San Pedro en el departamento del Valle.

La Registraduría nacional busca a futuro la masificación de la biometría, en todos los procesos electorales que se lleven a cabo dentro del territorio Nacional.

Sin embargo el gobierno Nacional encontró que los trámites o servicios que son solicitados por ciudadanos colapsan el funcionamiento de las entidades públicas, razón por la cual el 10 de enero de 2012 se publicó el decreto 019 correspondiente a la ley anti trámites.

Para el funcionamiento de esta ley, la Registraduría Nacional del Estado Civil, en compañía del Ministerio de Telecomunicaciones, determinaron que para la solicitud de un trámite o servicio se requería de la plena identificación de la persona.

Esto llevó a que se implementará el uso de la biometría de huella dactilar, como sistema de identificación de personas, en donde se acotejará la identidad de un individuo contra la base de datos de la Registraduría Nacional del Estado Civil; además de esto *"el sistema de identificación automatizada AFIS, tiene la capacidad de verificar los datos reales de más de 38 millones de Colombianos vivos y muertos por medio de la captura y cotejo de la huella dactilar"* [8], [9].

Otras de las implementaciones que se han generado con la biometría de huella dactilar, ha sido el servicio que lanzó la Cámara de Comercio de Bogotá junto con Certicamara, llamado "Huella dactilar certificada", la cual verifica y certifica la identidad de un individuo por medios electrónicos, contra la base de datos del gobierno nacional.

"Esta herramienta hará posible también que entidades del Estado, puedan implementar servicios más eficientes para el ciudadano como: trámites, certificados a domicilio, atención en otras zonas del país con dispositivos biométricos y sin la presencia de funcionarios de la entidad. Especialmente, podrá erradicar la suplantación de identidad". [10]

Estas soluciones han sido de gran ayuda para mitigar el riesgo de suplantación de identidad, y se convierten en un procedimiento clave, para mejorar la protección de datos personales en Colombia.

VII BIOMETRÍA DE HUELLA DACTILAR PARA EL SECTOR PRIVADO

Este sector ha utilizado este tipo de biometría en su mayoría para dos fines; el primero de ellos el control de acceso, con el cual se limitan o permiten que las personas puedan acceder a lugares físicos o virtuales restringidos por su nivel dentro de la organización; el segundo uso fue otorgado como un control de asistencia, en donde el trabajador debe poner su huella dactilar sobre un lector a la entrada y a la salida de sus labores.

Bajo cualquiera de los modelos anteriores se implementan logs sobre las bases de datos, que le permiten a los empleadores llevar un control muy asertivo de lo que sus trabajadores hacen en sus organizaciones.

Cabe resaltar que la ley 1581 del 2012 la cual hace referencia a la protección de datos personales, establece en su artículo quinto que los datos biométricos son datos sensibles y para ser almacenados deben ser solicitados con autorización explícita del titular además debe ser protegida por sistemas seguros.

VIII. HACKING Y FORENSE EN DISPOSITIVOS BIOMÉTRICOS DE HUELLA DACTILAR

Uno de los grandes problemas que enfrenta cualquier tecnología de seguridad es cuando se implementa un control digital, siempre los delincuentes informáticos están pensando en cómo comprometerlo.

A pesar que las huellas tienen patrones únicos que hacen que la probabilidad de que haya dos huellas iguales entre 2 seres humanos sea muy baja, es posible realizar una copia física de la huella de una persona, con el uso y practica de técnicas de adquisición de huellas dactilares de tipo forense convencional y digital.

Básicamente en la actualidad, encontramos tres formas principales de comprometer la seguridad de los dispositivos para la recepción de huellas dactilares:

La primera forma es la utilizada por cualquier persona para identificarse en sistemas de información, esta consiste en que el individuo de manera voluntaria realiza una copia de su huella en una goma con la finalidad de poder darle su huella a otras personas cuando esta no se encuentra cerca del sistema de autenticación; este método es muy utilizado en el sector privado con el fin de saltarse los controles de acceso o controles de asistencia por ejemplo:

Aprovechándose de un nivel jerárquico alto en la compañía "Un alto funcionario que quiere hacerle ver la junta directiva que es una persona cumplidora de sus obligaciones, se aprovecha de un trabajador de nivel inferior para que coloque su huella dactilar en el lector biométrico de asistencia".

La segunda forma tiene que ver con la aplicación de métodos forenses convencionales para obtener la huella dactilar de una persona sin consentimiento de la misma; el uso de esta técnica tiene dos connotaciones, la primera es utilizada por organismos de investigación los cuales cuentan con toda la infraestructura y tecnología para la obtención de huellas digitales de manera legal. La segunda se remonta a métodos forenses artesanales como el polvillo de carbón, en donde un delincuente puede hacer una copia de la huella dactilar, dejada en espejos, envases, picaportes, vidrios, acetatos, pantallas de computadores, tabletas, celulares, y muchas otras superficies planas, que son las que hacen que la huella conserve toda su forma; puesto que en superficies rugosas este tipo de procedimiento, no sería tan exacto ya que se necesita como mínimo del 75% de la totalidad de la huella, para que esta pueda ser acotejada.

Y la tercera forma, se deriva de la segunda pero difiere en que esta utiliza métodos tecnológicos para su obtención. Dígase por la suplantación del hardware "Cambiando el dispositivo de lectura biométrico", de software "Cuando se compromete la base de datos en donde se almacena la información de la huella", a través de ataques informáticos

Una vez que la huella es obtenida se procede a realizar un molde en un material maleable, con el fin de utilizarlos en los dispositivos de uso biométrico. [11]

En Colombia se ha constatado que estas técnicas se adquieren por un costo muy bajo e incluso realizando búsquedas a través de internet en donde se explica a detalle como violentar estos sistemas de adquisición de huellas dactilares, lo que genera un panorama de inseguridad muy alto para este tipo de biométricos.

IX. SEGURIDAD ENTORNO A BIOMETRÍA DE HUELLA DACTILAR

Dado el impacto que ha tenido la violación de estas tecnologías en el campo biométrico, las investigaciones han llevado a realizar estudios sobre huelleros dactilares de dedo vivo, los cuales además de ver la geometría de la huella, detectan que por las pequeñas venas de los dedos circule constantemente sangre, bajo un rango normal de temperatura; con lo cual se evitaría que se realicen moldes de las huellas. Teniendo en cuenta la perversidad de la mente humana y sobre de los delincuentes, una forma de vulnerar este sistema, seria cortar el dedo del usuario para poder acceder al sistema y como este aun conserva las propiedades e impulsos eléctricos, el delincuente puede autenticarse y comprometer el sistema.

Sin embargo, "*investigadores de Dermalog Identification Systems en Alemania desarrollaron un escáner que puede diferenciar entre tejido vivo y muerto"* [12]. Esta técnica consiste en que cuando al dedo se le aplica presión sobre una superficie este se vuelve blanco puesto que la sangre se retira por un momento; los investigadores detectaron que cuando un dedo vivo es colocado sobre un lector biométrico, la luz absorbida es menor que cuando se le ejerce presión, mientras que con un dedo muerto este no muestra esta alteración.

Gracias a los avances mostrados por la ciencia, las entidades públicas y privadas de Colombia comienzan a tener nuevos mecanismos de protección, contra los ciberdelincuentes que intentan comprometer los sistemas de información, basados en biométricos de huellas dactilares.

X. CONCLUSIONES

Hoy en día una de las principales razones de la implementación de biométricos, en las diferentes entidades, son los constantes ataques ejecutados por delincuencia común o hackers contra la seguridad de la información; relación causa - efecto que hace que los sistemas permanezcan a la vanguardia, ante el reto de mantener una seguridad perimetral óptima.

Hasta la fecha ningún dispositivo de uso biométrico dactilar, garantiza que no pueda ser vulnerado, por lo tanto para mejorar la seguridad de los mismos es necesario acompañarlos de otros métodos de autenticación como lo son: lo que la persona puede tener "Un Token", lo que la persona sabe "Una Contraseña" y lo que la persona es "Una combinación con otras tecnologías biométricas, como puede ser el reconocimiento de iris, entre otras".

En Colombia la biométrica de huella dactilar y la puesta en marcha de la nueva legislación de datos personales, ofrecerá herramientas de seguridad más efectivas, para controlar la identificación de personas en los sistemas de información que minimizaran el riesgo de suplantaciones.

Uno de los retos que tiene la biometría en el futuro es apuntarle a desarrollar una nueva técnica, que ofrezca niveles de seguridad más altos, como podría ser el caso de un patrón que la persona tiene, pero no conoce y que a su vez no es constante.

XI. REFERENCIAS

[0] Sergio Paños Hernández (2010-06-19). Tecnologías biométricas aplicadas a la seguridad. [En línea]. Disponible en http://www.slideshare.net/serweb/presentacion-biometra

[1] [3] Domingo Morales L. Javier Ruiz del Solar (2000). Sistema biométricos: Matching de huellas dactilares mediante transformada de Hough generalizada. [En línea]. Disponible en: http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

[2] Gits informática. Seguridad informática y delitos telemáticos (2003). Biometría, criptografía y riesgos. [En línea].Disponible: http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

[4] Grupo Atenea. (2011). Biometría informe. [En línea]. Disponible en: http://www.revistatenea.es/RevistaAtenea/REVISTA/PDF/Documentos/Documento_650.pdf

[5] Universidad Nacional Autónoma De México. Facultad de Ingeniería. Clasificación de los sistemas biométricos. [En línea]. Disponible en: http://redyseguridad.fi-p.unam.mx/proyectos/biometria/clasificacionsistemas/recohuella.html

[6] Juan Carlos Santamaria Olivares. (2008). Reconocimiento y validación de huellas dactilares utilizando una red neural. [En línea]. Disponible en: http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista_tecnologia/volumen7_numero1/reconocimiento_validacion_huellas_dactilares7-1.pdf

[7] Diario el País. (2013) Cuatro años de biometría en Colombia son todo un éxito. [En línea]. Disponible en: http://www.elpais.com.co/elpais/colombia/noticias/cuatro-anos-biometria-colombia-son-todo-exito-registraduria

[8] Registraduría Nacional del estado civil. (2012) La huella dactilar: la base del sistema de identificación en Colombia. [En línea]. Disponible en: http://www.registraduria.gov.co/rev_electro/2012/rev_elec_noviembre/revista_noviembre2012.html#10

[9] Carlos F. Reisz. (2010) Foro de seguridad. Identificación dactiloscópica. [En línea]. Disponible en http://www.forodeseguridad.com/artic/discipl/4112.htm

[10] Certicamara. (2013) CCB y Certicamara lanzaron servicio de huella dactilar certificada. [En línea]. Disponible en: http://camara.ccb.org.co/contenido/contenido.aspx?conID=11647&catID=380

[11] Alesteir. (2010). Como vulnerar un sistema de biometría-Huellas dactilares. [En línea]. Disponible en: http://locvtvs.blogspot.com/2010/07/como-vulnerar-un-sistema-de-biometria.html

[12] Fayerwayer (2011). Inventan un escáner de huellas digitales que distingue entre vivos y muertos. [En línea]. Disponible en: http://www.fayerwayer.com/2011/07/inventan-un-escaner-de-huellas-digitales-que-distingue-entre-vivos-y-muertos/

Autores:

Andrés Camilo Castelblanco Peñuela
Ingeniero de sistemas de la Escuela Colombiana de Ingeniería.
Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia.
Gerente de tecnología.
Dreamtechlogic – Zipaquirá 2013

Ángela María Medina Gutiérrez
Ingeniera de Sistemas de la Fundación Universitaria Juan de Castellanos.
Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia.
Asesora tecnologías de la información y comunicación.
Alcaldía de Tibasosa – Boyacá 2013.