¿QUÉ TAN SEGUROS SON LOS DATOS BIOMÉTRICOS?

Viteri Riascos Yenifer Andrea
Cundinamarca, Universidad Piloto de Colombia
Bogotá, Colombia
yeniferviteri@gmail.com

Resumen **–** A través de este documento se dará a conocer acerca de la biometría, con los distintos tipos que existen hasta el momento, así como también las fases que tiene para su procesamiento.

Se proporcionará una breve explicación de la transformada de la HAAR que es la modalidad con que las imágenes y el iris utilizan para procesar la información y así poderla comparar con la base de datos.

Por último habrá una ilustración de la legislación que cubre este tipo de datos en Colombia, si es considerado un dato sensible o no.

Índice de Términos **–** Transformada de la HAAR, criptobiometría, datos sensibles, transformada de Fourier.

Abstract – Through this document will be unveiled on biometrics, with the different types that exist so far, and also phase that has to be processed.

A brief explanation will be provided of the HAAR transform that is the modality with which the images and iris used to process the information and so it can be compared with the database.

Finally there will be an illustration of the law covering this type of data in Colombia, if deemed sensitive or not data.

Keywords – The HAAR transform, criptobiometría, sensitive data, Fourier transform.

I. INTRODUCCIÓN

En la actualidad, la biometría es considerada como uno de los métodos más seguros para identificar a un individuo, ya que compara partes físicas y/o de comportamiento, que aunque en algunas ocasiones son similares, existe algún mínimo detalle que las hace únicas.

Para muchos, esta tecnología hace algunos años solo se podía ver por las películas o en las grandes empresas que invertían una gran cantidad de dinero en estos métodos.

Sin embargo, el primer dispositivo que se conoció para hacer uso de este método, se creó en el año de 1.883 y era un sistema antropométrico que se encargaba de medir las partes del cuerpo y de identificar algunas marcas o tatuajes que presentará una persona.

Aunque esto empezó hace mucho tiempo atrás, sólo hasta el siglo XIX la cultura occidental comenzó a ponerlo en práctica y aunque a lo largo de estos años ha tenido un desarrollo evidente, todavía presenta fallas que no permiten la exactitud de esta información.

Uno de los tipos de captura de datos biométricos que presenta mayor desarrollo tecnológico es la huella dactilar, ya que hoy en día es posible encontrar dispositivos a muy bajo precio y que son de gran precisión.

Tanto que ahora las empresas lo usan mucho, ya sea para el ingreso de personas a áreas restringidas,

también al momento de hacer un registro o consulta de información en algún aplicativo, o simplemente para monitorear los horarios de entrada y salida de su sitio de trabajo.

No obstante es un método que puede ser fácilmente falsificable, debido a que con ciertos elementos puede crear un copia de la huella, es por eso que los otros tipos biométricos, se consideran más seguros y de mayor impacto.

II. BIOMETRÍA

La biometría es un tipo de tecnología que se encarga de analizar los datos biológicos, para convertirlos en una secuencia numérica; estás secuencias se realizan mediante un proceso de comparación entre plantillas y un algoritmo, estos dependen de la modalidad biométrica que se desee almacenar.

Esta tecnología es muy utilizada en diferentes empresas con múltiples propósitos, por ejemplo, brindar la seguridad en el acceso a sitios restringidos, recopilar el tiempo de ingreso a la empresa u otros sitios, o por el contrario descontarlo para no tener que estar padeciendo de fraude, así como también se usa para identificar a una persona en algún aplicativo bancario u otro que traía la información del usuario.

En la actualidad existen dos clases de biometría, la estática que se encarga de las características físicas del individuo, y la dinámica que se basa en el comportamiento del individuo, cada una de ellas cuenta con diferentes tipos de reconocimiento:

TABLA I.
CLASES DE BIOMETRÍA

Estática	Dinamica
Huella Dactilar	Escritura manuscrita
Iris	Voz
Geometría de la mano	Gesto
Retina	Caminar
Rostro	Movimiento corporal
Líneas de la mano	Tecleo

Nota: Adaptado de “Nuevas Tecnologías Biométricas – Informaticas”, por M. De Vincenzi y M.Semeria, 2015, p. 5 [1]

También existe la biometría multimodal que es capaz de analizar diferentes tipos de datos biométricos, ya sea huella e iris, voz y cara, entre otras posibles mezclas.

El poder aplicar esta modalidad le asegura a la empresa o al individuo tener un nivel más alto de seguridad en su información, porque va a tener que pasar por dos parámetros. Y pese a que este método sería el de mayor seguridad en la actualidad, solo existen aplicativos que usan la biometría monomodal, ocasionando un nivel inferior a lo que este podría ser.

Ya que si se requiere poner en práctica dos patrones biométricos se deben hacer uso de un programa por cada uno de ellos.

Sin embargo, el proceso de funcionamiento de estos aplicativos trabaja de forma estándar para cualquiera de las dos modalidades.

Para cada uno de estos tipos de identificación biométrica, existe una serie de etapas que permiten el funcionamiento de cada una ellas:

- **Captura:** En esta etapa se obtienen los datos del individuo, ya sean estáticos o dinámicos para proporcionarlos al aplicativo que va a realizar el reconocimiento.

- **Pre-Procesado:** Aquí se procede a localizar y adecuar las muestras tomadas, extrayendo el contenido necesario para utilizar en la siguiente etapa y así poder procesar la muestra.

- **Extracción de Características:** Una vez que la muestra esté ajustada a los requerimientos de esta etapa, se pasa por el algoritmo que extrae la información a comparar con la base de datos que se tiene.

- **Comparación:** Por último se realiza la comparación entre el resultado del algoritmo y la información almacenada en la base de datos.

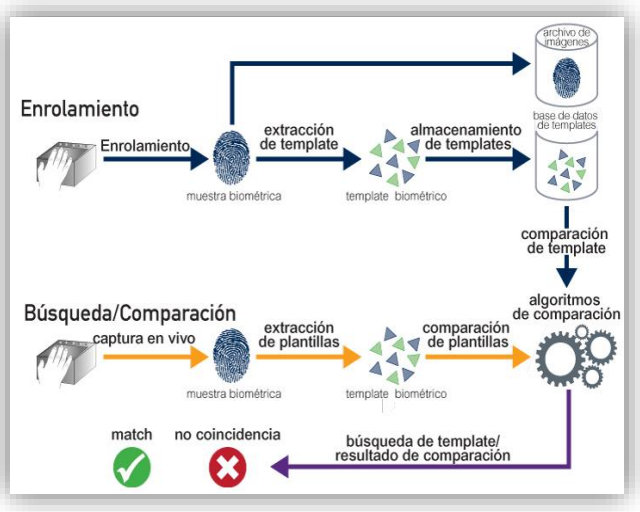

Figura 1. Proceso de la Biometría
http://www.aware.com/es/biometrics/whitepapers/wab_biometric-processes.html

En la figura 1 se evidencia el proceso por el cual pasan los datos biométricos, cabe resaltar que en la etapa de extracción se determina el algoritmo dependiendo del tipo de datos biométrico, por ejemplo para la extracción de imágenes o del iris, uno de los algoritmos más utilizados es la transformada de HAAR.

Ya que su base se fundamenta en la transformada de Fourier y está a su vez en la teoría de ondículas para el análisis de señales o de ondas en este caso.

III. TRANSFORMADA DE HAAR

Esta transformada proviene de la transformada de Wavelet la cual se usa para codificar señales, en donde se logra definir algunas zonas de las imágenes, ya sean de un computador o de una cámara fotográfica.

Las trasformada de HAAR es un algoritmo propuesto para la comparación de imágenes, debido a que al utilizarlo permite obtener algunas características de las imágenes.

Este algoritmo se basa en matrices que son ortogonales, y solo usan tres operaciones matemáticas básicas; sumar, restar y dividir. A continuación se relaciona un ejemplo de este procedimiento por medio de un vector.

- Vector: [7 3 16 4 5 9 8 10]

Paso 1. Media:

- ✓ (7 + 3) / 2 = 5
- ✓ (16 + 4) / 2 = 10
- ✓ (5 + 9) / 2 = 7
- ✓ (8 + 10) / 2= 9

Vector Resultado: [5 10 7 9]

Paso 2. Diferencias:

[**7** 3 **16** 4 **5** 9 **8** 10] - [5 10 7 9]

(2 6 -2 -1)

Vector Resultado 1: [5 10 7 9 **2 6 -2 -1**]

Paso 3. Media + Diferencia:

[5 10 7 9 **2** 6 **-2** -1]

- ✓ (5 + 10) / 2 = 7,5
- ✓ (7 + 9) / 2 = 8

Vector Resultado 2: [7,5 8 2 -2 2 6 -2 -1]

Paso 4. Media + Diferencia:

[7,5 8 2 -2 2 6 -2 -1]

- ✓ (7,5 + 8) / 2 = 7,75

Vector Resultado 3: [7,75 2 2 -2 2 6 -2 -1]

Paso 5. Multiplicación de Vectores

Transformada de HAAR: VR1 * VR2 * VR3

[31/4 2 2 -2 2 6 -2 -1]

Los valores a usar en este algoritmo se encuentran en las plantillas que anteriormente se mencionaban, dependiendo de la configuración requerida por cada

aplicativo se determinará el número de bytes en el cual se va a almacenar la imagen.

Estos datos se capturan de forma hexadecimal, se aplica la transformada de HAAR y de acuerdo a la similitud que arroje, se compara con las otras plantillas almacenadas en la base de datos y se establece un porcentaje de similitud.

Ahora bien, este método ayuda considerablemente a la biometría, porque la matemática es el medio que asegura que los datos obtenidos sean exactos, sin embargo puede ocurrir que algún intruso altere está información en su trayectoria. Por tal motivo sería de gran ayuda que estos datos viajen por medio de la red de forma cifrada.

IV. CRIPTOBIOMETRÍA

Hoy en día la biometría se considera uno de los medios más seguros, debido a que se enfoca en datos únicos e irrepetibles de los individuos, sin embargo así como avanza su nivel de desarrollo también evoluciona la manera de quebrantar esta tecnología.

Ya que para muchos, los datos que son irrelevantes para los atacantes son valiosos, por ejemplo el método que se expuso en el punto anterior, porque solo toma ciertas partes de las imágenes y las otras las desechan, es aquí cuando los atacantes toman provecho de estos "residuos" para poder reutilizarlos.

Y no solo es posible utilizar este método, porque existen más para plagiar la información, en su gran mayoría utilizan la transferencia, ya sea en el proceso de extracción o en el de verificación.

Por eso es de gran utilidad que los datos que viajan a través de la red vayan cifrados, sin embargo actualmente no existe un método desarrollado que permita encriptar la información biométrica.

Hasta el momento el único método que se conoce para cifrar está información consiste en aplicar una llave, pública o privada, dependiendo como se implemente en la organización o el individuo que lo requiera.

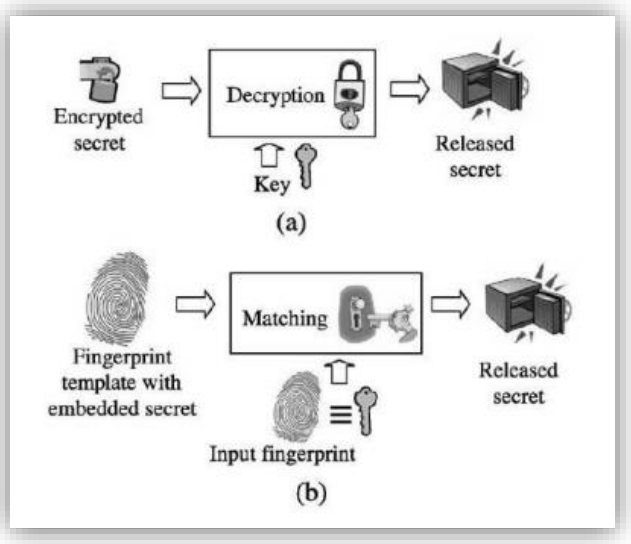

Figura 2. Cifrado de la Biometría
http://atvs.ii.uam.es/files/2006_PFC_Freire.pdf

No obstante se usa la manera de cifrar cualquier información, o sea con un software que dé encriptación y un software que escanee los datos biométricos a utilizar.

Sin embargo no es la más adecuada ya que lo correcto sería cifrar la información con un dato biométrico. Porque tan solo se está tomado la información biométrica capturada como cualquier dato que se requiera pasar por un dispositivo o por la red.

Pero al ser un dato sensible que puede ocasionar mucho daño a un individuo, sería de gran necesidad darle la seguridad que requiere.

Conforme a esta protección que se le puede generar a los datos biométricos, es importante dar a conocer que son datos sensibles, ya que al tener acceso a la base de datos donde se almacena está información, puede ocasionar discriminaciones o cualquier tipo de acción que afecte al individuo.

Es aquí donde se deben tener en cuenta las leyes que protegen la información, para que se empleen las medidas necesarias y no tener la eventualidad de

algún riesgo que los lleve a un acontecimiento legal.

V. LEYES DE PROTECCIÓN DE DATOS PERSONALES

Hasta hace algunos años en Colombia las empresas se dieron cuenta que la información era un activo importante, que no solo debían guardarla, sino que tenían que darle la seguridad necesaria para evitar pérdidas, alteraciones inadecuadas, plagio, entre otros sucesos que pueden ocurrir a lo largo del tratamiento de la información.

Adicional a esto, no solo es prioritario darle la seguridad para que la información se encuentre en buen estado, sino que también notaron que es importante que siempre esté disponible y no esté a la vista de cualquier individuo, ya que se puede hacer un uso inapropiado de ella.

Para el caso de la biometría debido a su naturaleza, en muchos países no es considerada como un dato sensible, debido a que para algunas naciones tan solo es un dato de acceso como una si fuera tarjeta de ingreso.

Sin embargo en Colombia si es considerado como un dato sensible, lo cubre la ley 1581 de 2012, en donde el artículo número cinco indica:

> **"Artículo 5°. Datos Sensibles**. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos."[11]

Está ley no solo les garantiza a los usuarios la seguridad de su información personal, sino que también obliga a las empresas que usen estos datos de manera adecuada y darle la prioridad que se requiere.

En muchas empresas no se consideraba está información como un dato importante, sino simplemente como si fuera cualquier tipo de información la cual se puede eliminar, distribuir, entre otros procesos por los cuales puede pasar.

De igual manera a este tipo de información también se acoge a la ley 1266 de 2008, que es la de habeas data, ya que la información se almacena en una bases de datos y se requiere que tenga una buena administración.

Porque en una de las principales entidades que tiene adaptada esta modalidad, con las bancarias y aquí no solo se encuentra la información financiera del individuo, sino también datos personales.

Los cuales por una posible falta de seguridad, si se genera un ataque y ocasiona alteración, perdida o divulgación, no solo puede afectar al individuo en la parte financiera, sino también en la psicológica. Debido a que en Colombia todavía existe mucha discriminación racial y de otro tipo de discriminación que perturba de manera crítica a la persona.

A raíz de todo esto es indispensable aplicar todas las medidas de seguridad que se encuentren avaladas en la actualidad, para tener la total certeza que el método el cual se esté aplicando sea totalmente seguro y no presente ninguna vulnerabilidad no contemplada.

VI. CONCLUSIONES

La Biometría es una tecnología que aunque lleva muchos años practicándose de distintas maneras no se le ha dado la seguridad e importancia necesaria.

Hasta hace algunos años, se identificó como un medio por el cual es difícil de suplantar a un individuo.

Sin embargo utiliza los métodos tradicionales para su almacenamiento, captura y envió, llevándola a tener las mismas debilidades que presenta cualquier dato.

El desarrollo se ha basado en cómo capturar y traducir estos datos en binarios para que sean comprensibles a un computador.

Si se logrará darle la importancia necesaria a está manera de identificar a un individuo, sería una de las más seguras. Debido a que el cuerpo humano tiene muchas partes únicas y de comportamiento que no se repiten en ningún ser humano, caso contrario a los métodos utilizados actualmente.

Sin embargo se considera que una gran debilidad de esta tecnología sería la vejez, ya que con el pasar de los años el cuerpo cambia y va perdiendo ciertos factores.

Como por ejemplo la huella dactilar o la forma de las manos, porque estás se van arrugando y en muchos casos se encojen.

Por esa razón se creé que aunque los avances han sido de manera abismal, todavía falta dar seguridad para este tipo de sucesos.

Adicionalmente la criptobiometría tan solo se contempla como un término y no se tiene en la actualidad un método que permita aplicar el cifrado de la información con estos datos.

VII. REFERENCAS

[1] Dr Marcelo De Vincenzi, Ing Marcelo Semeria, “Nuevas Tecnologías Biométricas – Informáticas” https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CC0QFjAC&url=http%3A%2F%2Fwww.biometria.gov.ar%2Fmedia%2F14089%2FUAI.ppt&ei=6h52VfCGO8PWsAWwn4LICw&usg=AFQjCNGldazzTnJp-9ZfckxogCsfcpHLQg&sig2=D70HQN4Pgk2KADU6q0aYRQ&bvm=bv.95039771,d.b2w
Ene 25 2015

[2] “Transformada De Haar (Hat)” http://alfonsomartin.es/tdi/pdf/haar.pdf

[3] Margaret Rouse, “Biometría” http://searchdatacenter.techtarget.com/es/definicion/Biometria
Oct 2008

[4] Aware, "¿Qué es la biometría? - Documentos informativos" http://www.aware.com/es/biometrics/whitepapers/wab_biometric-processes.html

[5] Homini, "Plataforma Biométrica Homini" http://www.homini.com/new_page_5.htm
2004

[6] El Mundo, "Qué son los datos biométricos" http://www.elmundo.es/espana/2013/12/05/52a0749d63fd3d8c498b456b.html
Dic 05 2013

[7] L.A. Ruiz, A.A. Boriskevich, V.Yu. Tsviatkou, "Metodo para el cálculo bidimencional de la transformada wavelet Haar de domenes basada en una recursiva permutacion–Z" http://servicio.bc.uc.edu.ve/ingenieria/revista/v18n3/art03.pdf
Dic 29 2011

[8] Kimaldi, "Encriptación Biométrica" http://www.kimaldi.com/area_de_conocimiento/biometria/encriptacion_biometrica

[9] Manuel Ricardo Freire Santos, "Desarrollo de un Criptosistema Biometrico Basado en Firma Manuscrita" http://atvs.ii.uam.es/files/2006_PFC_Freire.pdf Jun 2006

[10] El Congreso de la República, "Ley Estatutaria No. 1266 de 2008" http://www.sic.gov.co/drupal/sites/default/files/files/ley1266_31_12_2008(1).pdf Dic 31 2008

[11] El Congreso de la República, "Ley Estatutaria 1581 DE 2012" http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Autor
Yenifer Andrea Viteri Riascos
Ingeniera de Sistemas
Est. Especialización en Seguridad Informática
Seminario de Gestión de la Seguridad y el Riesgo
Universidad Piloto De Colombia
Junio 2015