Autenticación Biométrica: Estado del arte

Juan Manuel Alvarez[#1], Nicolás Campuzano[*2], Luis Castro Peralta[#3],
Juan David Garcia[#4],Wilson Piravaguen[#5]

[#]*Departamento de Ingeniería de Sistemas e Industrial,*
Universidad Nacional de Colombia sede Bogotá

[1]jmalvarezd@unal.edu.co

[2]ncampuzanoa@unal.edu.co

[3]lfcastrop@unal.edu.co

[4]judgarciani@unal.edu.co

[5]wapiravaguens@unal.edu.co

***Abstract*— Authentication as a means of identifying a person such that we are able to discern the resources to which that person has access to has been a point of increasing interest as information grows in importance. Biometric Authentication allows us to discern a human being by very specific physiological characteristics. This paper describes the currently public-available means of Biometric Authentication, the state of the art on Biometric Technology (anno 2018), and a look into the future of Biometric Authentication as the world-wide adopted way of ensuring information security.**

***Keywords*— Biometrics, Authentication, Iris, Fingerprint, Face**

I. Introducción

La autenticación biométrica es conocida como el proceso de vincular una característica física o comportamental en pro de identificar y dar acceso a las personas en diferentes sistemas, igualmente, se conoce como el sistema más robusto para la autenticación, ya que sigue la filosofía de "lo que usted es" sobreponiéndose a "lo que usted tiene" o "lo que usted sabe.

Históricamente estos sistemas de seguridad se asocian a costos altos de adquisición, implementación y mantenimiento, sin embargo con el avance tecnológico en los dispositivos móviles específicamente en cámaras, sensores y procesadores, se ha logrado una democratización de los sistemas de autenticación biométrica para los usuarios finales e inmersos en este contexto actual, es de importancia conocer el estado del arte de los diferentes mecanismos de biometría.

II. Características de un indicador biométrico

Para identificar cuáles son los indicadores o características que permiten crear un sistema robusto de autenticación biométrica se necesitan los siguientes cuatro factores:

Universalidad: Todos los individuos de la población tienen la característica o comportamiento a medir.

Unicidad: La existencia de que dos individuos o personas tengan una característica idéntica, es ínfima o despreciable. Se entiende por una característica idéntica, cuando el sistema autentica de manera errónea a una persona confundiéndose con otro individuo.

Permanencia: A través del tiempo la característica no puede cambiar drásticamente para que el sistema no identifique de manera correcta al individuo.

Cuantificación: La característica se puede medir por medio de hardware o método algorítmico para dar como resultado una medida que puede ser guardada y comparada en la correcta identificación y autenticación.

III. Métodos de autenticación biométrica

Análisis del iris: Es un método de autenticación biométrica que es aplicado a través de la captura en una imagen del iris de la persona, no debe ser confundido con el análisis de retina, ya que este es una técnica que analiza únicamente los patrones de los vasos sanguíneos de la retina.

Su uso depende de una cámara la cual captura en detalle la estructura del iris, la mayoría de los sistemas que usan este método capturan una imagen en una longitud de onda cercana al infrarrojo (Near Infrared Wavelength)[2] NIW por sus siglas en inglés, esto se debe a que los iris de color más oscuro sólo revelan su estructura con suficiente calidad en este rango de ondas.

Este método cumple con los factores de un indicador biométrico, el iris es una característica muy consistente, el reconocimiento de los patrones puede ser aplicado hasta 30 años luego del registro de dicho patrón con facilidad ya que este, aunque visible en una persona está protegido del medio ambiente, entre otras ventajas del método está que es relativamente simple de usar.

Entre las desventajas el mayor riesgo de un posible engaño del escáner por las bajas resoluciones que manejan estos dispositivos, es posible que sean engañados por fotos muy detalladas o por un iris falso, distintas técnicas como el verificar si el iris reacciona a los cambios de luz han sido una solución parcial a este tipo de ataques.

Firma manuscrita: Es un método que se basa en la forma particular de escribir de las personas, esta es relativamente única y difícil de imitar, por esta razón ha tenido importancia a la hora de desarrollar sistemas basados en esta característica.

La firma se ha aceptado como una forma de autenticación clásica, la mayoría de personas tienen una firma y con ello se clasifica como un método de autenticación de "algo que sé", con la llegada de la era digital se puede agregar más características a la firma que solo su forma, una estrategia que toman estos sistemas es tener como entrada para sus análisis no solo la imagen del escrito si no también la presión con la cual se hizo el trazo, un análisis dinámico también usa factores como el ritmo, tiempo de escritura y presión en cada trazo, esto hace más preciso el método, aunque una firma luzca simple él intentar imitarla se convierte en un proceso bastante complejo cuando se incluyen estos factores, sistemas que solo se basan en la forma de la firma están en desuso [2], dada la facilidad para el atacante de falsificar la firma.

Su implementación requiere de una pantalla táctil que sea sensible a la presión, la mayoría usa un stylus ya que las firmas escritas con un dedo en una pantalla táctil comprometen la precisión del método.

Huella dactilar: Los patrones de huella dactilar son dados por las marcas de las crestas papilares que se encuentran en los dedos, estos patrones tienen las características de ser detallados, únicos, permanentes e inmutables durante la vida de una persona, haciéndolos adecuados como medida biométrica a largo plazo[1].

En el pasado la huella dactilar se obtenía haciendo uso de tinta y papel, pero hoy en día se obtiene principalmente a través de medios electrónicos, estos usan técnicas basadas en principios ópticos, térmicos, de ultrasonido o de capacitancia, siendo este último uno de los más utilizados en los dispositivos móviles actuales.

Dado el creciente mercado de teléfonos inteligentes con sensores de huella dactilar, el uso de este sistema es cada vez más frecuente, su uso se basa principalmente en desbloquear el teléfono móvil sin embargo cada vez son más las aplicaciones de banco o de datos sensibles que lo usan como método de autenticación. A pesar de ser una técnica biométrica bastante utilizada enfrentada algunos desafíos, ya que los sensores pueden llegar a verse afectados por factores como la humedad y la suciedad, además de poder ser engañados por huellas dactilares artificiales de plastilina obtenidas a partir de un molde de la huella real.

Reconocimiento facial: El reconocimiento facial es la aplicación de técnicas computacionales para la identificación de una persona a partir de una imagen o una grabación de vídeo, esta tecnología extrae diferentes características faciales, como por ejemplo la posición, tamaño y forma de la nariz, boca, mentón y ojos, además de las distancias entre estos, para finalmente compararlas con las plantillas almacenadas en una base de datos.

El reconocimiento facial comparado con otras tecnologías biométricas se queda corto en términos rendimiento[2], es por eso que se han estado desarrollando muchas técnicas para su implementación, como el uso de sensores 3D, cámaras térmicas, análisis de textura de la piel y una gran variedad de algoritmos, todos esto buscando obtener la mayor precisión posible, haciendo de este una campo que se encuentra en amplio desarrollo.

En la actualidad este sistema es cada vez más usado gracias a los avances en cámaras y sensores de los teléfonos móviles, uno de los más destacados es el sistema de Face ID desarrollado por Apple, el cual en su módulo de reconocimiento genera un mapa 3D de la cara utilizando más de 30.000 puntos de infrarrojos en la cara del usuario.

El reconocimiento facial es uno de los sistemas más sensible a la privacidad, ya que las imágenes del rostro brindan más información acerca de las personas, como puede ser su género, etnia y edad.

Escaneo de la retina: Es un método de autenticación biométrica que se ejecuta dirigiendo un rayo de luz infrarroja de baja energía hacia el ojo de una persona cuando ésta mira a través de un escáner.

La retina humana es un tejido compuesto por células situadas en la parte posterior del ojo, es única ya que posee una estructura compleja de las venas capilares que suministran la sangre a la retina.

La red de vasos sanguíneos es tan compleja que ni siquiera dos gemelos idénticos tienen el mismo patrón. Los patrones de la retina pueden verse alterados en caso de glaucoma, diabetes o trastorno degenerativo de la retina, aún así, usualmente estos patrones se mantienen sin variación desde el nacimiento hasta la muerte.

Debido a que los vasos sanguíneos dentro de la retina absorben la luz más rápidamente que el tejido circundante, se varía la cantidad de luz utilizada durante el escaneo produciendo diferentes patrones que posteriormente son convertidos a código informático y guardado en una base de datos para su posterior uso.

Reconocimiento de voz: Del mismo modo que es posible identificar a una persona mediante el análisis de sus características faciales, se puede realizar mediante el análisis de su voz. La voz humana es simplemente un sonido, por lo que puede ser tratada como una señal más.

Este sistema trata de comprobar la identidad de una persona mediante la obtención y posterior comparación de la huella vocal del usuario, ésta es obtenida al hacer una captura dinámica de las características de la voz, como el agudo, la edad, el timbre o si es masculina o femenina mientras la persona habla, el sistema también determina el canal por el cual se está hablando, para establecer el posible grado de distorsión al que es sometido.

El reconocimiento de voz puede ser dependiente o independiente de texto. Es dependiente cuando el sistema sabe con anterioridad lo que la persona va a decir, por ejemplo si se tiene alguna contraseña en específico; es independiente de texto cuando la persona puede decir cualquier cosa y el sistema puede identificar al usuario.

IV. Autenticación multifactor

La autenticación por solo un factor es el uso de un solo método para verificar la identidad de una persona, ha sido adoptado por la sociedad por su simpleza y facilidad de uso para el usuario, estos sistemas aunque eficaces en su labor son débiles a distintos tipos de ataques especializados para cada método que usa en el reconocimiento[5], dado esto la autenticación por múltiples factores o MFA, por sus siglas en inglés, ha tomado papel en los últimos años para proveer un mayor nivel de seguridad en los sistemas y facilitar la protección de servicios y recursos críticos.

La autenticación biométrica ha sido una contribución significativa al modelo MFA, y ha aumentado su desempeño haciendo más difícil el suplantar a un individuo, el desafío más difícil de este tipo de sistema es el tomar una decisión entre los distintos parámetros que se reciben.

Una primera aproximación es la decisión secuencial en la cual el fallo en uno solo de los parámetros usados da como negada la autenticación de los usuarios, este método sufre de en la

característica de usabilidad ya que los distintos parámetros para la autenticación tienen distintos factores de error en sus mediciones facilitando los falsos negativos en una lectura.

Por otra parte, están los sistemas que usan un estimador para dar un factor de confiabilidad de cada parámetro y procesarlos para poder obtener la decisión final.

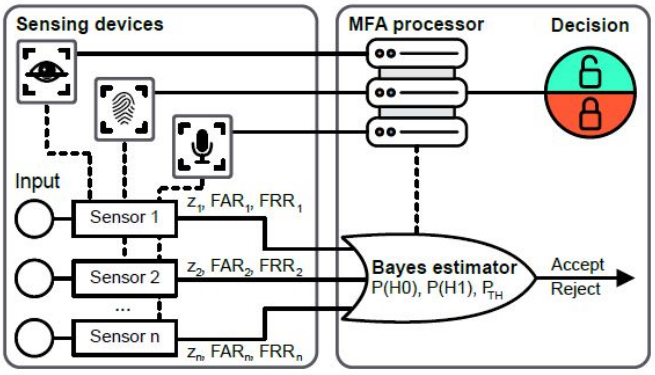

Fig. 1 Esquema de un sistema con estimador bayesiano para la toma de decisiones[5].

V. El futuro de la autenticación biométrica

Sin importar el método que se elija, a la hora de tomar la decisión de implementar un acercamiento a la autenticación biométrica, la limitante de mayor importancia será su rendimiento en situaciones reales. Al día de hoy, este rendimiento se ve afectado por distintos factores, entre ellos la calidad de los sensores, la velocidad de cálculo de los procesadores, incluso el nivel de adopción previo de una tecnología. A futuro, estos factores seguirán evolucionando, haciéndose más eficientes y confiables, lo que abrira la puerta a metodos de autenticacion cada vez mas sofisticados.

Actualmente, sistemas biométricos cognitivos están siendo desarrollados para usar la respuesta cerebral a estímulos de olor, percepciones faciales o rendimiento mental para autenticación en áreas de alta seguridad. En el futuro, una estrategia lo suficientemente refinada podría tomar raíces y reemplazar nuestros métodos más comunes de autenticación[1].

VI. Conclusiones

La autenticación biométrica es un campo en constante trabajo porque presenta uno de los retos más importantes para la actualidad, busca hacer cálculos complejos de manera óptima y a bajo costo, con el fin de crear una cercanía con los usuarios finales a través de incluir sistemas biométricos en su cotidianidad, principalmente, en sus teléfonos móviles. Con la familiaridad a los sistemas biométricos, podemos esperar que las entidades públicas y privadas requieran una implementación de estos en sus sistemas, por lo cual, la demanda de personal capacitado en su diseño y aplicación en escenarios reales se encontrara en un crecimiento que será necesario suplir.

Por otro lado, las políticas de protección de datos para las aplicaciones que contienen la información biométrica de sus usuarios deben ser exigentes y claras, dado que, esta información es de carácter sumamente sensible. Aunque los niveles de seguridad se aumenten considerablemente, es una responsabilidad profesional tener un trato adecuado de la información biométrica, no solo por quienes desarrollan los sistemas, sino por todos los actores participantes.

Por último, existirá una tarea retadora y exigente, cuando los sistemas de autenticación biométrica sean la cotidianidad en seguridad, para aquellos que deseen encontrar vulnerabilidades y fallos provechosos, pues repetir las condiciones naturales, únicas e intrínsecas de los humanos es una tarea de gran complejidad.

References

[1] Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology, 2(3), 13-28.

[2] Oostdijk, M., van Velzen, A., van Dijk, J., & Terpstra, A. State-of-the-Art in Biometrics for Multi-Factor Authentication in a Federative Context.

[3] Llopis, R.(s.f.) Sistemas De Autenticación Biométricos Seguridad Y Protección De La Información. Recuperado de http://spi1.nisu.org/recop/al01/llopis/Biometricos.PDF

[4] Biometrics: authentication and identification (2018) por Gemalto. Recuperado de https://www.gemalto.com/govt/inspired/biometrics

[5] Ometov, A., Bezzateev, S., Mäkitalo, N., Andreev, S., Mikkonen, T., & Koucheryavy, Y. (2018). Multi-Factor Authentication: A Survey. *Cryptography*, *2*(1), 1.

[6] Reconocimiento de iris y escaneo de retina ¿Son lo mismo? (s.f.). Recuperado de https://www.by.com.es/blog/reconocimiento-de-iris-y-escaneo-de-retina/