Biometría informática y su aplicación a la seguridad

Pablo Soëtard García

20-12-2019

EPS - UAM

Índice

Origen y evolución de la Biometría

La palabra biometría viene del griego bios (vida) y metron (medida), se define como el proceso de tomar medidas estandarizadas y únicas de seres vivos o procesos biológicos.

Desde la antigüedad los seres humanos hemos hecho uso de rasgos biométricos para reconocernos y establecer relaciones entre nosotros, estos eran rasgos como la cara o la voz.

La primera referencia a técnicas biométricas para la identificación de individuos se remonta al siglo VIII en la antigua China, donde hacían uso de huellas dactilares en documentos y esculturas de arcilla para denotar la autoría de las obra.
En el año 1000 DC. fue la primera vez que se usaron huellas dactilares para resolver un crimen, y 600 años después se realizó el primer estudio exhaustivo de huellas dactilares.

A finales del siglo XIX se concluyó que las huellas dactilares eran rasgos biométricos únicos para cada humano, esto condujo a que muchos departamentos de policía empezasen a almacenar huellas de delincuentes con el fin de cotejarlas con aquellas encontradas en escenas de crímenes. Y en 1986, sir Alec Jeffreys utilizó por primera vez el ADN para identificar al autor de unos asesinatos en Inglaterra.

En los últimos años, gracias al avance de las tecnologías modernas, nos encontramos técnicas de identificación biométrica en nuestro día a día. Con dichos avances hemos desarrollado dispositivos capaces de detectar rasgos biométricos tales como las huellas dactilares, rasgos faciales o el iris. Gracias a la reducción de los costes de producción y la globalización, dichos dispositivos se encuentran integrados en dispositivos personales tales como nuestros teléfonos inteligentes.
Por ello estas tecnologías futuristas ya no pertenecen tan solo al mundo de la ciencia ficción o incluso de las corporaciones gubernamentales o empresas punteras, sino que son accesibles para todo el público. Esto se puede observar en la Figura 1.

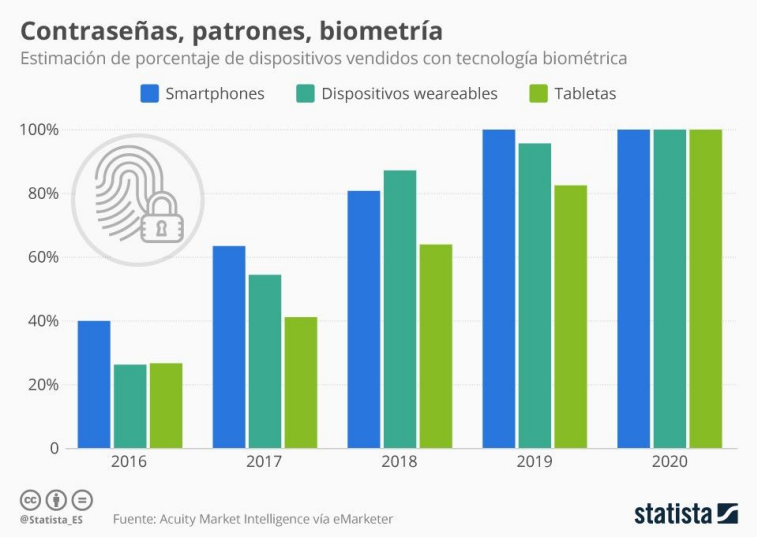

Figura 1

Biometría y biología

Todos los sistemas biológicos tienen rasgos biométricos, es decir, propiedades de dichos seres de las que se pueden sacar medidas, patrones…etc

No todos los rasgos biométricos son aptos para usarlos en técnicas de identificación de individuos, por ejemplo, si tuviéramos dos seres, uno humano y otro indefinido, y quisiéramos determinar si el segundo pertenece a la especie humana al igual que el primero. Podríamos hacer uso de técnicas biométricas para resolver nuestro problema, pero para ello deberíamos encontrar un rasgo biométrico válido, es decir, uno que fuese común a toda la especie humana pero no se diese en otras especies. Un ejemplo de rasgo biométrico no válido para nuestro problema sería la altura, si medimos al primer individuo, y comparamos esa medida con la obtenida del segundo, seguramente obtengamos que las medidas difieren, esto se debe a que la altura no es un rasgo biométrico único para la especie humana.

Los rasgos biométricos se pueden clasificar en dos categorías, fisiológicos y conductuales, además según su naturaleza pueden ser:

- Universales: se da en todos los individuos, sin distinción
- Únicos: rasgo distinguible en cada individuo
- Permanentes: rasgo que se mantiene de forma contínua

- Mediciones fisiológicas:

Este tipo de rasgos pueden ser morfológicos o biológicos. Algunos de los rasgos morfológicos más populares son: las huellas dactilares, la forma de la mano, el iris, la forma de la cara… etc. Por otro lado algunos rasgos biológicos son: el ADN, la sangre, la saliva o en general cualquier fluido de un indivíduo.

- Mediciones conductuales:

Las formas más comunes son el reconocimiento de voz, la dinámica de la firma (velocidad de movimiento del bolígrafo, aceleraciones, presión ejercida, inclinación), la dinámica de la pulsación de las teclas, la manera en que se utilizan los objetos, la forma de andar, el sonido de los pasos, los gestos… etc.

Sin embargo, los diferentes tipos de mediciones no tienen el mismo nivel de confiabilidad. Las medidas fisiológicas ofrecen un mayor grado de confianza ya que no depende en gran medida del estado de individuo y se consideran generalmente permanentes, al contrario que los rasgos conductuales, que pueden variar a lo largo de la vida del individuo.

Funcionamiento de sistemas biométricos aplicados a la seguridad

Los sistemas biométricos actuales están basados en la tecnología y se suelen instalar en dispositivos electrónicos con el el fin de aumentar su seguridad.

La base de funcionamiento de un sistema biométrico es la comparación de una representación digital de un rasgo biométrico con otro previamente guardado del mismo tipo. Por lo que un sistema biométrico es básicamente un sistema de reconocimiento de patrones que reconoce a individuo basándose en sus rasgos biométricos.

Un sistema biométrico suele estar compuesto por cuatro módulos principales, el primero un sensor. Este es el módulo que usa el sistema biométrico para digitalizar los rasgos biométricos de los usuarios, este sensor depende del tipo de rasgo biológico que se quiera capturar, por ejemplo, para reconocimiento facial una cámara sería un buen sensor para el sistema biométrico.
El segundo módulo es el que se encarga de obtener patrones de los datos digitalizados de los rasgos biométricos obtenidos con el sensor, por lo que de una cantidad muy alta de datos que han sido recogidos por el sensor obtenemos un conjunto más reducido que contiene la información necesaria para realizar la identificación del usuario.
El tercer módulo es la base de datos, donde se encuentran guardados los rasgos biométricos digitalizados de los individuos a identificar.
Por último, el cuarto módulo se encarga de encontrar una equivalencia entre el rasgo digitalizado del usuario obtenido en el segundo módulo, y aquellos que se encuentran guardados en la base de datos.

Para hacer uso de estos sistemas biométricos se deben de seguir una serie de pasos, primero se tiene que realizar un proceso de registro que se compone de las siguientes fases:

- Captura: se digitalizan los datos biométricos del usuario mediante un sensor.
- Procesamiento: de esta digitalización se extraen ciertas características personales y se crea un modelo con ellas.
- Inscripción: se almacena este modelo de forma que se pueda autenticar a dicho usuario en el futuro mediante el sistema biométrico.

Posteriormente, en el proceso de autenticación se digitaliza un rasgo biométrico del usuario mediante el sensor y se compara con aquellos ya guardados en el sistema, esto se puede realizar de dos formas diferentes:

- Identificación: se compara el rasgo biométrico con todos aquellos guardados en el sistema biométrico. Esto es una tarea con un alto coste computacional.

- Verificación: consiste en comparar el rasgo biométrico del usuario con tan solo uno de los guardados en el sistema, con el fin de verificar que el usuario es quien dice ser.

Antes de utilizar un sistema biométrico hay que establecer unos parámetros en el, estos parámetros son los siguientes:

- Tasa de Falsa Aceptación (FAR): Esta es la probabilidad de que el sistema biométrico vincule una muestra biométrica de un usuario con alguna de las que tiene guardadas, aunque los individuos no sean los mismos. Sus valores suelen oscilar entre 0.0001% y 0.1% para ser aceptables.

- Tasa de Falso Rechazo (FRR): Es la probabilidad de que el sistema no vincule a un individuo con su muestra biológica ya almacenada en él. Sus valores suelen estar entre el 0.00066 % y el 1 % para ser aceptables.

- Tasa de Error Equitativa (EER): es el punto de corte de las dos anteriores y corresponde a una indicación de que el sistema biométrico funciona correctamente, esto se puede observar en la Figura 2. Cuanto menor sea este valor, mejor será el sistema biométrico con respecto a su seguridad y eficacia.

- Tiempo de comprobación: Es el tiempo que tarda el sistema biométrico en procesar una muestra biométrica, bien sea aceptando o rechazando dicha muestra. Este se considera aceptable siempre que se mantenga por debajo de los 2 segundos.

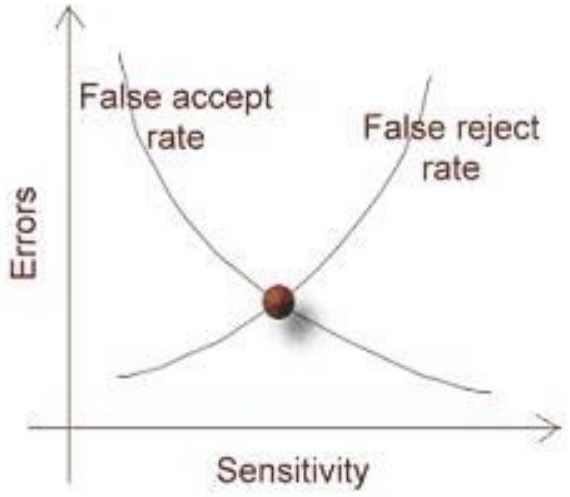

Figura 2

Para que un sistema biométrico pueda identificar correctamente las muestras biométricas que se le dan, este debe ser capaz de extraer información de ellas. Aquí entra en juego la habilidad del sistema para el reconocimiento de patrones. Normalmente se utilizan algoritmos que extraen rasgos locales de los datos biométricos y con ellos generan un identificador asociado a esos datos con tal de comparar ese identificador con el previamente guardado.
Hoy en día se están empezando a implementar algoritmos de deep learning para la fase de reconocimientos de patrones de los sistemas biométricos. Con estos nuevos métodos de aprendizaje automático se están consiguiendo sistemas de seguridad biométricos mucho más versátiles y seguros.

Tipos de sistemas de seguridad biométricos

Existen diferentes tipos de sistemas de seguridad biométricos, dependiendo de el tipo y número de muestras que necesiten para autenticar al usuario.

Según el tipo de muestra biométrica que necesite el sistema, podemos distinguir entre:

- Sistemas de biometría estática: estos sistemas hacen uso de rasgos biométricos estáticos. Algunos ejemplos de sistemas biométricos estáticos son los lectores de huellas dactilares, geometría de la mano, reconocimiento de iris o facial.
  Todos ellos tienen un rasgo en común, una vez han obtenido la muestra biométrica estos solo deben de obtener sus patrones y compararla con aquellas muestras que mantienen guardadas. Debido a la naturaleza estática de la muestra biométrica, los sistemas no deben realizar más procesamiento que el de obtener patrones de ella.

- Sistemas de biometría dinámica: estos sistemas obtienen como muestra biométrica un rasgo dinámico. Los más populares son los de reconocimiento de voz, dinámica de firma manuscrita o dinámica de teclado.
  Estos sistemas son más complejos de configurar ya que estos rasgos biométricos pueden verse afectados según el estado anímico del usuario.

Según el número de muestras biométricas que necesite el sistema de seguridad biométrico para identificar a su usuario podemos distinguir dos tipos de arquitecturas de sistemas biométricos:

- Sistemas biométricos simples: son aquellos que solo requieren de una muestra biométrica de un solo tipo para autenticar a los usuarios.
  Algunos ejemplos de sistemas biométricos simples son los lectores de huellas dactilares, presentes en teléfonos inteligentes u ordenadores, que solo necesitan que el usuario se identifique con su huella para desbloquearse.

- Sistemas multibiométricos: estos sistemas se componen de varios sistemas biométricos simples. Su función es ofrecer un mayor grado de seguridad, debido a que requieren varias muestras biométricas distintas del el mismo usuario para identificarlo. Por ello es mucho más difícil vulnerar a todos los sistemas a la vez para que un usuario sea autenticado pese a que en un principio no debiera serlo.
  Estos sistemas se dan principalmente en el mundo de la empresa, ya que los usuarios individuales no suelen requerir de tal nivel de seguridad.

Vulnerabilidades y ataques a sistemas biométricos

Los sistemas de seguridad biométricos, como cualquier otro sistemas informático, son susceptibles a ataques y hackeos.

Estos ataques que pueden sufrir los sistemas de seguridad biométricos se pueden clasificar en tres categorías principales:

- Administrativos: son aquellos que se realizan desde dentro del sistema, mediante las credenciales del administrador. Estas credenciales pueden haber sido obtenidas por el atacante, por ejemplo mediante algún método de ingeniería social.

- Infraestructura no segura: como ya comentamos anteriormente, los sistemas biométricos están compuestos por módulos. Si el atacante es capaz de ganar control de alguno de esos módulos, por ejemplo mediante una vulnerabilidad en su firmware, será capaz de manipularlo de tal manera que podría tener control total del sistema de seguridad biométrico.

- Ataques adversarios: este tipo de ataques se basa en la creación de muestras biométricas artificiales con las que se intenta engañar al sistema de seguridad biométrico con el fin de que las tome como buenas y autentique el acceso.
  Estas muestras biométricas, por lo general, se generan partiendo de la información biométrica de un usuario real ya registrado en el sistema biométrico.

Para intentar mitigar estos ataques se puede optar por un sistema multibiométrico, que es mucho más difícil de vulnerar, ya que dispone de muchos subsistemas biométricos a los cuales se tendría que ganar acceso simultáneamente para autenticar al atacante.

Si solo disponemos de un sistema de seguridad biométrico, para mitigar los ataques administrativos y de infraestructura, la única solución es aumentar el control de calidad de los sistemas, haciéndolos infranqueables ante ataques similares.
Por otro lado, nos queda la forma de solventar los ataques adversarios con muestras biométricas artificiales. Una de las técnicas más usadas es la medida de la temperatura del usuario a autenticar, al ser un humano quien debería de proporcionar la muestra biométrica, y al estar los humanos a una temperatura de unos 36º, los sensores de reconocimiento facial o huella dactilares suelen contar con algún método para obtener la temperatura del usuario, para así, de alguna manera, cerciorarse de que es un ser vivo.
Otra de las técnica usadas como medida preventiva para ataques de muestras biométricas artificiales que se usa en el reconocimiento facial son las cámaras de infrarrojos, que permiten obtener la profundidad de la imagen y así no autenticar una fotografía de un rostro en vez de un rostro real.

Últimamente se está haciendo uso de técnicas de inteligencia artificial y deep learning para entrenar modelos que son capaces de discernir entre muestras biométricas genuinas y artificiales, obteniendo resultados sorprendentes.

Conclusión

Como se ha podido ver, la biometría aplicada a la seguridad es una tecnología muy poderosa y práctica. Los sistemas biométricos, con el avance de la tecnología, se han hecho cada vez más baratos, y esto a permitido que estén al alcance de todos.

Pero no todo son ventajas, con algunos rasgos biométricos, uno puede deducir datos personales del usuario al que pertenece la muestra sin que él haya dado el consentimiento expreso de darlos. Por ello las empresas deben hacer un uso responsable de los datos de los usuarios que tienen, y más si van íntimamente ligados a su estado anímico, como son en este caso las muestras biométricas.

Además, se han visto diferentes ataques a los que son vulnerables los sistemas de seguridad biométricos, pese a que se esté trabajando en distintos métodos para mitigar dichos ataques, es conveniente concluir que este campo de la tecnología tiene un gran potencial pero queda mucho por investigar para conseguir sistemas de seguridad biométricos que funcionen a la perfección y sean infranqueables ante ataques.

Referencias

- Alejandro Alcalde, A. A. (2017, 23 septiembre). Biometría Aplicada a La Seguridad - Introducción. Recuperado 1 octubre, 2019, de https://elbauldelprogramador.com/biometria-seguridad-introduccion/

- Alejandro Alcalde, A. A. (2017, 8 octubre). Biometría Aplicada a La Seguridad - Sistemas Biometricos. Recuperado 1 octubre, 2019, de https://elbauldelprogramador.com/sistemas-biometricos/

- Cristina Heredia, C. H. (2017, 20 octubre). Biometría Aplicada a La Seguridad - Reconocimiento De Patrones. Recuperado 1 octubre, 2019, de https://elbauldelprogramador.com/biometria-seguridad-patrones/

- La biometría aplicada a la seguridad. (2012, 31 septiembre). Recuperado 2 octubre, 2019, de https://tuinterfaz.mx/articulos/8/64/la-biometria-aplicada-a-la-seguridad/

- Biometría aplicada a la salud y a la seguridad. (2013, 1 julio). Recuperado 2 octubre, 2019, de https://www.investigacionyciencia.es/blogs/tecnologia/20/posts/biometra-aplicada-a-la-salud-y-a-la-seguridad-11242

- Florencia Gomez Forti, F. G. F. (2018, 15 enero). Biometría aplicada a la seguridad informática. Recuperado 2 octubre, 2019, de https://www.itsitio.com/ar/biometria-aplicada-la-seguridad-informatica/

- El Economista. (2005, 20 mayo). Biometría aplicada en sistemas de seguridad. Recuperado 2 octubre, 2019, de http://www.belt.es/noticias/2005/mayo/20/biometria.asp

- Luis Moreno, L. M. (2019, 13 mayo). La Biometría en la vida cotidiana: Seguridad en tu vida diaria. Recuperado 2 octubre, 2019, de http://biometriaaplicada.com/sitio/la-biometria-en-la-vida-cotidiana-seguridad-en-tu-vida-diaria/

- Asem Othman, A. O. (2018, 19 julio). What Is A Biometric System, and How To Secure It | Veridium. Recuperado 3 octubre, 2019, de https://www.veridiumid.com/blog/biometric-system-secure/

- IFSEC Global. (2019, 14 mayo). Biometric security systems: a guide to devices, fingerprint scanners, facial recognition, access control. Recuperado 3 octubre, 2019, de https://www.ifsecglobal.com/global/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/

- SrinivasaRao SubramanyaRao and Enrique Argones Rua, S. S. E. A. (2019, 3 octubre). Comments on a recently proposed Privacy Preserving Lightweight Biometric Authentication System for IoT Security. Recuperado 4 octubre, 2019, de https://arxiv.org/pdf/1910.01446.pdf

- Yi Zeng, Enmeng Lu , Yinqian Sun , Ruochen Tian, Y. Z. (2019, 19 septiembre). Responsible Facial Recognition and Beyond. Recuperado 4 octubre, 2019, de https://arxiv.org/pdf/1909.12935.pdf

- ANIL K. JAIN AND ARUN ROSS, A.K. (2004, 1 enero). Multibiometric systems. Recuperado 4 octubre, 2019, de https://paginas.fe.up.pt/~ee03106/Relatorio/Referencias/5.pdf

- Parvathi Ambalakat, P. A. (s.f.). Security of Biometric Authentication Systems. Recuperado 4 octubre, 2019, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.9610&rep=rep1&type=pdf

- Javier Ortega García, J. O. G. (2008, 1 mayo). Biometría y Seguridad. Recuperado 5 octubre, 2019, de https://www.researchgate.net/profile/Fernando_Alonso-Fernandez/publication/280722075_Seguridad_Biometrica/links/55c2ce5308aeca747d5dd882.pdf

- Universidad Tecnológica de Pereira. (2010, 1 diciembre). SISTEMAS DE SEGURIDAD BASADOS EN BIOMETRÍA. Recuperado 5 octubre, 2019, de https://www.redalyc.org/pdf/849/84920977016.pdf

- Anjith George, Zohreh Mostaani, David Geissenbuhler, Olegs Nikisins, Andre Anjos and Sebastien Marcel, A. G. (2019, 19 septiembre). Biometric Face Presentation Attack Detection with Multi-Channel Convolutional Neural Network. Recuperado 5 octubre, 2019, de https://arxiv.org/pdf/1909.08848.pdf

- Lazaro J. González-Soler, Marta Gomez-Barrero, Leonardo Chang, Airel Pérez-Suárez, Christoph Busch, L. J. G. (2019, 27 agosto). Fingerprint Presentation Attack Detection Based on Local Features Encoding for Unknown Attacks. Recuperado 6 octubre, 2019, de https://arxiv.org/pdf/1908.10163.pdf

- ANDREW JASON SHEPLEY, A. J. S. (2019, 12 julio). Face Recognition in Unconstrained Conditions: A Systematic Review. Recuperado 6 octubre, 2019, de https://arxiv.org/pdf/1908.04404.pdf

- Sobhan Soleymani, Ali Dabouei, Jeremy Dawson, and Nasser M. Nasrabadi, S. S. (2019, 8 agosto). Defending Against Adversarial Iris Examples Using Wavelet Decomposition. Recuperado 6 octubre, 2019, de https://arxiv.org/pdf/1908.03176.pdf