Análisis de la eficiencia de las tecnologías biométricas en la seguridad de información

Analysis of the Efficiency of Biometric Technologies in Information Security

Angello Paul García Charcape [1]
Miriam Maryori Horna Maguiña [2]
Alberto Carlos Mendoza De Los Santos [3]

DOI: *https://doi.org/10.26495/qa023w39*

Resumen

En la actualidad, se tienen una gran variedad tecnologías biométricas que se utilizan en la seguridad de la información, por lo que en la revisión sistemática se hace un análisis de cuatro tipos de tecnologías biométricas: reconocimiento de huellas dactilares, facial, de iris y de voz; para reconocer cuales son las más seguras y eficaces en diferentes contextos. En el proceso de llevar a cabo la revisión, se empleó la metodología PRISMA, lo que nos permitió identificar 16 artículos científicos publicados en los últimos 6 años, siguiendo los criterios de selección y exclusión. Los resultados mostraron que cada tecnología biométrica tiene sus ventajas y desventajas, dependiendo del nivel de precisión, invasión, resistencia al fraude y facilidad de uso que requiera la aplicación de seguridad. Se concluye que no existe una tecnología biométrica óptima para todos los casos, sino que se debe elegir la más adecuada según las necesidades y condiciones específicas de cada contexto.

Palabras clave
Reconocimiento facial, reconocimiento de huella dactilar, reconocimiento de iris, reconocimiento de voz, tecnología biométrica.

Abstract
Currently, there is a wide variety of biometric technologies that are used in information security, so in the systematic review an analysis of four types of biometric technologies is carried out: fingerprint, facial, iris and voice recognition; to recognize which are the safest and most effective in different contexts. In the process of carrying out the review, we used the PRISMA methodology, which allowed us to identify 16 scientific articles published in the last 6 years, following the selection and exclusion criteria. The results showed that each biometric technology has its advantages and disadvantages, depending on the level of precision, invasiveness, fraud resistance and ease of use required by the security application. It is concluded that there is no optimal biometric technology for all cases, but rather the most appropriate one must be chosen according to the specific needs and conditions of each context.

Keywords:
Facial recognition, fingerprint recognition, iris recognition, voice recognition, biometric technology.

[1]*Universidad Nacional de Trujillo, Trujillo – La Libertad, Perú, t023300420@unitru.edu.pe*
[2]*Universidad Nacional de Trujillo, Trujillo – La Libertad, Perú, t513300720@unitru.edu.pe*
[3] *Universidad Nacional de Trujillo, Trujillo – La Libertad, Perú, amendozad@unitru.edu.pe*

1. INTRODUCCIÓN

La biometría es un método que posibilita la identificación de individuos a partir de características físicas o de comportamiento únicas. Con el progreso de la tecnología, los procesos de reconocimiento biométrico se han automatizado y perfeccionado, especialmente en el ámbito de la seguridad. Estos métodos son ampliamente empleados en la identificación forense, la administración de identidades y el control de acceso en instituciones tanto públicas como privadas, estas tecnologías se basan en gran medida en el procesamiento de datos. En la era actual de la transformación digital y el uso creciente de dispositivos electrónicos, la seguridad de la información es crucial. Las tecnologías biométricas, que posibilitan la identificación de individuos a través de rasgos físicos distintivos como las huellas dactilares y el reconocimiento facial, han adquirido un rol fundamental en la seguridad de la información.

Según Mejía (2020) indica que las tecnologías biométricas son sistemas automáticos empleados para identificar a individuos mediante el análisis de sus rasgos físicos o de comportamiento. Algunas de las tecnologías biométricas comúnmente utilizadas en el campo de la seguridad incluyen:

- El reconocimiento de huellas dactilares: Según la revista Biometrics (2023) el reconocimiento de huellas dactilares es una técnica biométrica que se utiliza en la seguridad para identificar a una persona a través de sus huellas dactilares. Biometrics nos dice que esta técnica se basa en la singularidad de las huellas dactilares, que son únicas para cada individuo y ayuda a las organizaciones para evitar la duplicación o falsificación de identidades.

- El reconocimiento facial: Según Astudillo (2020) el uso de tecnología para identificar a individuos por sus características faciales se conoce como reconocimiento facial en seguridad. Esta tecnología cuenta con una diversidad de usos en el ámbito de la seguridad, que abarcan desde el control de acceso a edificios hasta la localización de personas que están evadiendo la justicia.

- Reconocimiento de iris: Segun Devincenzi (2012) el reconocimiento de iris es una técnica de autenticación biométrica que se basa en las intrincadas estructuras del iris del ojo de una persona para confirmar o verificar su identidad. Este método es particularmente útil para identificar a personas que están privadas de su libertad, ya que no requiere contacto físico entre el dispositivo y la persona que se está identificando.

- Reconocimiento de voz: Según la página Shaip (2023) la tecnología del reconocimiento de voz ha sido creada para identificar, decodificar, diferenciar y autenticar la voz de un individuo basándose en su huella de voz única. En el contexto de la seguridad, esta tecnología se emplea para autenticar transacciones, controlar el acceso, autenticar a los usuarios de la banca telefónica a larga distancia y supervisar para prevenir el uso indebido de la información.

El propósito de esta revisión sistemática consiste en evaluar la efectividad de las tecnologías biométricas en la seguridad de la información, así determinar cuáles son las más seguras y eficaces en diferentes contextos. Para ello, se realizará un análisis detallado de las investigaciones científicas existentes acerca del tema, con el fin de identificar las principales tendencias en este campo.

La justificación de esta revisión sistemática radica en la importancia de contar con información precisa y fiable acerca de las últimas tendencias en tecnologías biométricas aplicadas a la seguridad de la información, para poder tomar decisiones informadas y aumentar la eficiencia de los sistemas de seguridad. Además, esta revisión puede ser de interés para investigadores, profesionales y

organizaciones que se dedican al ámbito de la seguridad de la información y las tecnologías biométricas.

En este sentido, autores como Sun et al. (2021) menciona que la identificación biométrica tiene la ventaja única de ser distinta, estable, confiable y portátil. Sin embargo, también se destaca la importancia de analizar cómo funcionan las tecnologías biométricas en diversos entornos y condiciones para poder identificar las limitaciones en su implementación.

2. MATERIALES Y MÉTODOS

La presente revisión sistemática fue realizada con la metodología PRISMA. Esta metodología se desarrolló en cuatro fases ver Figura 1.

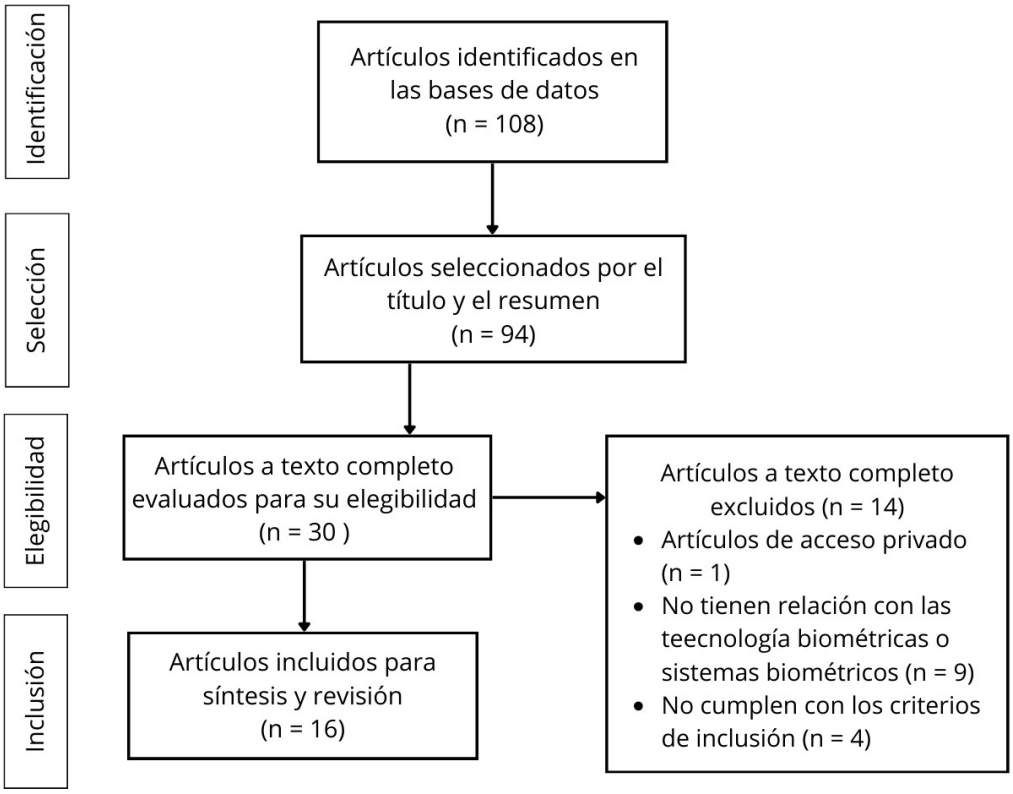

Figura 1. Diagrama de flujo de la metodología PRISMA.
Fuente: Elaboración propia.

En la fase de identificación, planteamos la pregunta de investigación ¿Cuáles son las tecnologías biométricas más eficientes en seguridad de la información? a partir de ahí se realizó una búsqueda de artículos en la base de datos ScienceDirect, Scielo y Google Académico. Se encontró 108 artículos al realizar una búsqueda lógica con los términos "Tecnología biométrica", "Seguridad de la información", "Reconocimiento facial", "Reconocimiento de huellas dactilares", "Reconocimiento de iris", "Reconocimiento de voz" que estaban incluidos en las palabras claves, títulos y resúmenes.

En la fase de selección, se omitieron 14 artículos repetidos, así quedaron 94 artículos.

En la fase de elegibilidad, analizando el título y el resumen se descartaron 64 artículos, quedando 30 artículos que tenían relación con el tema de investigación y que luego serían analizados a profundidad.

En la fase de inclusión, se consideraron los criterios de inclusión que son los artículos publicados desde el año 2018 al 2023 y artículos en español e inglés, además se excluyeron los artículos que no tenía relación con las "Tecnología biométricas" o "Sistemas de biométricos". Finalmente se consideraron 16 artículos para realizar la revisión.

3. RESULTADOS

Para la exploración y análisis detallado del tema de revisión sistemática, se identificaron 16 artículos en total, donde se mostrará la eficiencia de la tecnología biométrica. Después de realizar el análisis, se muestra el resumen en 4 tablas donde cada una contiene investigaciones referentes a una tecnología biométrica.

En la Tabla 1 se muestra un resumen de algunos artículos encontrados sobre el reconocimiento de huellas dactilares, sobre cómo fueron utilizadas. En la Tabla 2 se muestra un resumen de artículos encontrados sobre el reconocimiento facial donde resaltaron su facilidad de uso, para la Tabla 3 se muestra los artículos para el reconocimiento de iris donde destaca su alta seguridad y por último en la Tabla 4 están los resultados del reconocimiento de voz donde se habla de su bajo factor confiable en comparación a otros reconocimientos.

Reconocimiento de huellas dactilares

Tabla 1. Resultados del reconocimiento de huellas dactilares.

N°	Título del artículo	Resultados
1	Contactless Palmprint Recognition System: A Survey (2022)	La identificación de huellas es rápida y de reconocimiento único.
2	A hierarchical heterogeneous ant colony optimization based fingerprint recognition system (2023)	La verificación de huellas dactilares es rápida. Con el algoritmo HHACOFM puede hacer coincidir una huella digital de entrada con 17931 plantillas almacenadas en 4,4 segundos.
3	The PLUS Multi-Sensor and Longitudinal Fingerprint Dataset: An Initial Quality and Performance Evaluation (2022)	El rendimiento del reconocimiento de las huellas dactilares tiende a deteriorarse si se incluyen datos separados por períodos de tiempo. La calidad de las huellas digitales es reducida de las personas mayores.
4	Security and Accuracy of Fingerprint-Based Biometrics: a review (2019)	La precisión del reconocimiento de huellas dactilares es notable. En comparación con otros rasgos biométricos (rostro, iris y voz), los sistemas basados en reconocimiento de huellas dactilares son los que se implementan más ampliamente.

Fuente: Elaboración propia.

En la Tabla 1 se observa que los sistemas basados en este método son ampliamente implementados debido a su alta precisión y rapidez. Sin embargo, se encontró que la calidad de las huellas digitales puede deteriorarse en personas mayores, lo que podría afectar su eficacia en ciertos contextos.

Reconocimiento facial

Tabla 2. Resultados del reconocimiento facial.

N°	Título del artículo	Resultados
1	Face recognition: Past, present and future (a review) (2020)	El rendimiento de los métodos de reconocimiento facial que utilizan imágenes puede ser limitado. Algunas dificultades en el reconocimiento facial son las variaciones en la pose de la cabeza, la iluminación, la edad y las expresiones faciales así como la similitud entre los individuos.
2	A Survey on Face Recognition Techniques in Machine Learning (2022)	Los métodos convencionales para identificar rostros mediante algoritmos, el aprendizaje profundo Y los sistemas de reconocimiento facial que utilizan redes neuronales como base se caracterizan por una alta precisión de reconocimiento y un alto grado de automatización.
3	Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers (2019)	La tecnología de detección facial es asequible y no invasiva. El reconocimiento de iris y de huellas dactilares requieren dispositivos adicionales, pero el reconocimiento facial, dado que los teléfonos inteligentes ya tienen cámaras integradas, no requiere hardware adicional. La detección facial se destaca como uno de los escasos enfoques que ofrece una elevada exactitud con una mínima intrusión.
4	Multispectral Facial Recognition: A Review (2020)	El método de identificación, al ser automático, no requiere ninguna intervención del usuario, pero tiene la desventaja de que, si la base de datos es grande, este proceso puede llevar mucho tiempo.

Fuente: Elaboración propia.

En la Tabla 2 se muestra resultados del reconocimiento facial, destacando su conveniencia y facilidad de uso, especialmente debido a la ubicuidad de las cámaras integradas en dispositivos como teléfonos inteligentes. A pesar de ello, se identificaron limitaciones en el rendimiento de los métodos que utilizan imágenes, como las variaciones en la pose de la cabeza, la iluminación, la edad y las expresiones faciales, así como la similitud entre los individuos.

Reconocimiento del Iris

Tabla 3. Resultados del reconocimiento de iris.

N°	Título del artículo	Resultados
1	Sistema de acceso y control para el área de gestión documental por sistemas de reconocimiento biométrico (huella dactilar e iris) (2018)	El reconocimiento de iris tiene ventajas como su alta precisión, su estabilidad, su no invasividad y su resistencia al fraude.
2	Bibliometric Survey on Biometric Iris Liveness Detection (2020)	Los métodos basados en las características utilizan algoritmos para analizar las imágenes del iris capturadas por un escáner estándar y detectar artefactos falsos, es generalmente considerado un método de autenticación

		biométrica muy seguro debido a la singularidad del patrón del iris.
3	Relative Performance Analysis of Edge Detection Techniques in Iris Recognition System (2018)	el reconocimiento del iris es una tecnología biométrica de alta precisión y baja invasión que se utiliza para proteger activos altamente confidenciales y mejorar la seguridad global y el transporte
4	Security System Enhancement Using Iris Scan Biometric Technology for ATM Machine (2023)	El reconocimiento de iris es una forma fiable y efectiva de mejorar la seguridad de los cajeros automáticos, pero todavía necesita algunos avances para ser más preciso y fácil de usar.

Fuente: Elaboración propia.

En la Tabla 3 tenemos los resultados del reconocimiento de iris, donde destacó por su alta precisión, estabilidad, no invasividad y resistencia al fraude. Sin embargo, se reconoció la necesidad de mejorar la comodidad y conveniencia del usuario, así como reducir el ruido y la distorsión en las imágenes del iris para aumentar su precisión.

Reconocimiento de voz

Tabla 4. Resultados del reconocimiento de voz.

N°	Título del artículo	Resultados
1	Evaluación del reconocimiento de voz entre los servicios de Google y Amazon aplicado al Sistema Integrado de Seguridad ECU 911 (2021)	El reconocimiento de voz tiene un nivel de seguridad medio, ya que no es tan fiable como otros sistemas biométricos, como las huellas dactilares o el reconocimiento de iris.
2	Sistema de seguridad para el control de acceso a una vivienda mediante el reconocimiento de voz utilizando coeficientes cepstrum MFCC Y DTW (2019)	El sistema obtuvo un 95% de tasa de acierto en el reconocimiento de voz de los miembros del hogar, y un 100% de tasa de acierto ante intrusos, usando los métodos MFCC y DTW para la extracción de características y la comparación de señales, respectivamente.
3	MÉTODO DE SEGURIDAD EN UNA CARCEL MEDIANTE UN SISTEMA DE RECONOCIMIENTO DE VOZ EN MATLAB (2018)	Se han realizado pruebas con 10 usuarios registrados y 5 intrusos, usando dos palabras clave: apertura y cierre. Se han obtenido índices de acierto entre el 66% y el 73% para los usuarios registrados, y entre el 88% y el 89% para los intrusos.
4	A cascaded voice biometric system (2018)	El sistema en cascada en el reconocimiento de voz reduce la tasa de falsos positivos y aumenta la seguridad del sistema de reconocimiento biométrico. El sistema tiene una alta eficiencia de identificación, hasta aproximadamente el 91.2%.

Fuente: Elaboración propia.

En la Tabla 4 respecto al reconocimiento de voz si bien puede proporcionar autenticación para transacciones y control de acceso, no es tan confiable como otros sistemas biométricos debido a su susceptibilidad al ruido ambiental, los cambios en la voz y los ataques de suplantación.

4. DISCUSIÓN

Los resultados muestran que las cuatro tecnologías biométricas (reconocimiento de huellas dactilares, facial, de iris y de voz) tienen diferentes niveles de eficiencia y seguridad en la seguridad de la información, dependiendo del contexto y las condiciones de su aplicación.

La identificación de huellas dactilares representa una de las tecnologías biométricas más empleadas y exactas, ya que se basa en la singularidad de las huellas dactilares y puede prevenir la duplicación o falsificación de identidades (Biometrics, 2023; Yang et al., 2019). Sin embargo, esta tecnología puede tener algunas limitaciones, como el deterioro del rendimiento del reconocimiento con el tiempo o la reducción de la calidad de las huellas dactilares de las personas mayores (Kirchgasser et al., 2022).

La identificación de individuos a través de sus características faciales es posible gracias a la tecnología de reconocimiento facial, que es asequible y no invasiva dentro de las tecnologías biométricas (Aznarte, 2022; Zhang & Kang, 2019). Esta tecnología tiene un alto potencial para diversas aplicaciones de seguridad, como el control de acceso o la detección de fugitivos (Astudillo, 2020). Pero el reconocimiento facial también puede enfrentar algunos desafíos, como variaciones en la pose de la cabeza, la iluminación, la edad y las expresiones faciales, así como la similitud entre individuos (Taskiran et al., 2020; Shantanu et al., 2022).

El reconocimiento del iris es una tecnología biométrica altamente precisa y estable que utiliza las estructuras complejas del iris con el propósito de confirmar o establecer la identidad de una persona (Cañón y Cuellar, 2018; Devincenzi, 2012). Esta tecnología es adecuada para entornos de alta seguridad, como prisiones o cajeros automáticos, ya que es no invasiva y resistente al fraude (Mayare et al., 2023; Podder et al., 2018). El reconocimiento del iris también puede requerir algunas mejoras para ser más preciso y fácil de usar, como reducir el ruido y la distorsión en las imágenes del iris o mejorar la comodidad y conveniencia del usuario (Khade, 2020).

El reconocimiento de voz es una tecnología biométrica de seguridad media que puede verificar la identidad de una persona mediante el reconocimiento de su única huella vocal. Esta tecnología puede proporcionar autenticación para transacciones, control de acceso, banca telefónica y monitoreo (Vásconez et al., 2021). El reconocimiento de voz no es tan confiable como otros sistemas biométricos, como el reconocimiento de huellas dactilares o del iris, ya que puede verse afectado por factores como el ruido ambiental, los cambios en la voz o los ataques de suplantación (Vásconez et al., 2021).

Se recomienda realizar más investigaciones para evaluar la eficacia de las tecnologías biométricas en escenarios específicos como en las organizaciones, en casas inteligentes y así mejorar su implementación.

5. CONCLUSIONES

Los resultados muestran que cada tecnología biométrica tiene sus ventajas y desventajas, dependiendo del nivel de precisión, invasión, resistencia al fraude y facilidad de uso que requiera la aplicación de seguridad.

Por ejemplo, el reconocimiento de huellas dactilares es una tecnología biométrica muy precisa y rápida, lo que la hace ideal para aplicaciones que requieren una autenticación rápida y segura, como el acceso a edificios o dispositivos móviles. Por otro lado, el reconocimiento facial es una tecnología biométrica conveniente y fácil de usar, pero puede ser menos precisa en situaciones en las que la iluminación o el ángulo de la cara pueden afectar la calidad de la imagen. En cuanto al reconocimiento de iris, aunque es una tecnología biométrica muy efectiva para mejorar la seguridad de los cajeros automáticos, todavía necesita algunos avances para ser más preciso y fácil de usar. Por último, el reconocimiento de voz es una tecnología biométrica de seguridad media que puede verificar la identidad de una persona mediante el reconocimiento de su única huella vocal, pero puede verse afectado por factores como el ruido ambiental o los cambios en la voz.

La implementación de estas tecnologías biométricas en la seguridad de la información es una herramienta valiosa, pero es importante tener en cuenta sus limitaciones y evaluar cuidadosamente su aplicación en cada contexto específico.

Además, se sugiere que se siga trabajando en la mejora de la precisión y facilidad de uso de las tecnologías biométricas existentes, especialmente en el reconocimiento de voz y facial.
Con esto podemos concluir que no existe una tecnología biométrica óptima para todos los casos, sino que se debe elegir la más adecuada según las necesidades y condiciones específicas de cada contexto.

REFERENCIAS

Abdalrahman, R. S. A., Bölat, B., & Kahraman, N. (2018). A cascaded voice biometric system. *Procedia Computer Science*. https://doi.org/10.1016/j.procs.2018.04.334

Alausa, D. W., Adetiba, E., Badejo, J. A., Davidson, I. E., Obiyemi, O., Buraimoh, E., Abayomi, A., & Oshin, O. (2022). Contactless Palmprint Recognition System: a survey. IEEE Access, 10, 132483-132505. https://doi.org/10.1109/access.2022.3193382

Astudillo, J. G. (2020). *PLATAFORMA DE SERVICIOS DE RECONOCIMIENTO FACIAL PARA DETECCIÓN DE PRÓFUGOS DE LA JUSTICIA EN ECUADOR*. https://www.semanticscholar.org/paper/PLATAFORMA-DE-SERVICIOS-DE-RECONOCIMIENTO-FACIAL-DE-Astudillo-Mora/1bef6b7ad334687fa8ef83bcf37b7ddfff381f5d

Aznarte, J. L. (2022). *Sobre el uso de tecnolog as de reconocimiento facial en la universidad: el caso de la UNED*. https://www.redalyc.org/journal/3314/331469022016/html/

Biometrics, A. (2023). Reconocimiento de huellas dactilares. *Aware*. https://www.aware.com/es/reconocimiento-de-huellas-dactilares/

Cañón, O. I., & Cuellar Castro, A. (2018). *Sistema de acceso y control para el área de gestión documental por sistemas de reconocimiento biométrico (huella dactilar e iris)*. INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO.

Chambino, L. L., Silva, J. S., & Bernardino, A. (2020). Multispectral Facial Recognition: a review. IEEE Access, 8, 207871-207883. https://doi.org/10.1109/access.2020.3037451

De Catalunya, U. O. (2018, 29 enero). *Método de seguridad en una cárcel mediante un sistema de reconocimiento de voz en MATLAB*. http://hdl.handle.net/10609/73188

Devincenzi, J. A. (2012, 1 octubre). *Reconocimiento biométrico de iris en ambientes de alta seguridad*. http://sedici.unlp.edu.ar/handle/10915/23644

Enrique, O. Q. C. (2019b). *Sistema de seguridad para el control de acceso a una vivienda mediante el reconocimiento de voz utilizando coeficientes Cepstrum MFCC y DTW*. http://dspace.unitru.edu.pe/handle/UNITRU/15622

Khade, S. (2020). *Bibliometric Survey on Biometric Iris liveness Detection*. DigitalCommons@University of Nebraska - Lincoln. https://digitalcommons.unl.edu/libphilprac/4439/

Kirchgasser, S., Kauba, C., & Uhl, A. (2022). The PLUS Multi-Sensor and Longitudinal Fingerprint Dataset: an initial quality and performance evaluation. IEEE transactions on biometrics, behavior, and identity science, 4(1), 43-56. https://doi.org/10.1109/tbiom.2021.3104108

Mayare, M. A., Shah, O., & Singh, A. K. (2023). Security system enhancement using Iris scan biometric technology for ATM machine. *International Journal For Multidisciplinary Research*, *5*(4). https://doi.org/10.36948/ijfmr.2023.v05i04.5773

Mejía, A. (2023). *Las 4 principales tendencias en biometría para 2020*. Ventas de Seguridad. https://www.ventasdeseguridad.com/2020021111874/noticias/tecnologia/las-4-principales-tendencias-en-biometria-para-2020.html

Podder, P., Parvez, A. H. M. S., Yeasmin, M. N., & Khalil, M. I. (2018b). Relative performance analysis of edge detection techniques in iris recognition system. *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*. https://doi.org/10.1109/icctct.2018.8551023

Sarah-Lf. (2020, 11 julio). *El futuro con la tecnología biométrica – LaFlecha*. https://laflecha.net/el-futuro-con-la-tecnologia-biometrica/

Shaip. (2023). What is voice recognition: How it works, advantages, example | Shaip. *Shaip*. https://es.shaip.com/blog/voice-recognition-overview-and-applications/

Shantanu, J., Vrushaket, C., Rushikesh, C., Tanvesh, C., & Priyanka, S. (2022). A Survey on Face Recognition Techniques in Machine Learning. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(6), 50-66. https://doi.org/10.32628/CSEIT228558

Sreeja, N. K. (2023). A hierarchical heterogeneous ant colony optimization based fingerprint recognition system. Intelligent Systems with Applications, 17, 200180. https://doi.org/10.1016/j.iswa.2023.200180

Sun, Z., Li, Q., Liu, Y., & Zhu, Y. (2021). Opportunities and challenges for biometrics. En *Springer eBooks* (pp. 101-125). https://doi.org/10.1007/978-981-15-8342-1_6

Taskiran, M., Kahraman, N., & Erdem, C. E. (2020). Face Recognition: Past, Present and Future (A review). Digital Signal Processing, 106, 102809. https://doi.org/10.1016/j.dsp.2020.102809

Vásconez, J. J. P., Ortiz, C., Cordero, M. P. O., León, P. A. P., & Orellana, P. C. (2021). Evaluación del reconocimiento de voz entre los servicios de Google y Amazon aplicado al Sistema Integrado de Seguridad ECU 911. *Revista Tecnológica ESPOL*, *33*(2), 147-158. https://doi.org/10.37815/rte.v33n2.840

Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). Security and Accuracy of Fingerprint-Based Biometrics: a review. Symmetry, 11(2), 141. https://doi.org/10.3390/sym11020141

Zhang, W. K., & Kang, M. (2019). Factors affecting the use of Facial-Recognition Payment: An example of Chinese consumers. IEEE Access, 7, 154360-154374. https://doi.org/10.1109/access.2019.2927705