Ingeniería Investiga

Vol. 7, e1099, año 2025
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v7i00.1099

Artículo de revisión

Eficacia y limitaciones de los sistemas biométricos en la verificación de identidad: Una revisión sistemática

Effectiveness and Limitations of Biometric Systems in Identity Verification: A Systematic Review

Bruno Samir Bocanegra Chistama[1]
https://orcid.org/0000-0003-1463-8999

Fernando Arturo Fernández Salvo[2]
https://orcid.org/0009-0006-1631-0099

Alberto Carlos Mendoza De Los Santos[3]
https://orcid.org/0000-0002-0469-915X

Recibido: 10/11/2024
Aceptado: 02/12/2024
Publicado: 27/12/2024

[1,2,3]Escuela de Ingeniería de Sistemas, Universidad Nacional de Trujillo, La Libertad, Perú

E-mail: [1]t013300220@unitru.edu.pe, [2]ffernandezs@unitru.edu.pe, [3]amendozad@unitru.edu.pe

Facultad de Ingeniería
Publicación Oficial

Resumen

La digitalización y automatización crecientes demandan métodos avanzados y seguros para el control de acceso. Este estudio sintetizó herramientas de inteligencia artificial (IA) aplicadas en este campo, mediante una revisión de literatura en bases como Scopus, SciELO e IEEE Xplore, utilizando PRISMA y VOSviewer. El análisis bibliométrico identificó a China, India, Estados Unidos y Corea del Sur como líderes en investigación, destacando términos como machine learning, deep learning, criptografía y biometría, junto con tecnologías emergentes como blockchain e IoT. Machine learning y deep learning sobresalieron como técnicas predominantes, mientras que blockchain aportó transparencia en la gestión de datos sensibles. Sin embargo, desafíos como altos costos, dependencia de datos extensos y preocupaciones de privacidad limitan su implementación. Se recomienda explorar métodos híbridos, optimizar los modelos de IA y reducir la dependencia de datos para mejorar la seguridad y la adopción de estas tecnologías

Palabras clave: control de acceso; sistemas de seguridad; inteligencia artificial; biometría.

Abstract

Increasing digitization and automation demand advanced and secure methods for access control. This study synthesized artificial intelligence (AI) tools applied in this field, through a literature review in databases such as Scopus, SciELO and IEEE Xplore, using PRISMA and VOSviewer. The bibliometric analysis identified China, India, the United States and South Korea as leaders in research, highlighting terms such as machine learning, deep learning, cryptography and biometrics, along with emerging technologies such as blockchain and IoT. Machine learning and deep learning stood out as predominant techniques, while blockchain brought transparency in the management of sensitive data. However, challenges such as high costs, reliance on big data and privacy concerns limit its implementation. It is recommended to explore hybrid methods, optimize AI models and reduce data dependency to improve security and adoption of these technologies.

Keywords: access control; security systems; artificial intelligence; biometrics; artificial intelligence; biometrics.

1. Introducción

En la era digital, la seguridad y protección de la identidad se han convertido en prioridades para gobiernos, empresas y ciudadanos. A medida que la sociedad avanza hacia una mayor digitalización y los servicios se ofrecen cada vez más en línea, la autenticación de la identidad de los usuarios se ha vuelto indispensable para mitigar riesgos como el robo de identidad, el fraude y los accesos no autorizados (Ghadge, 2024). Tradicionalmente, los métodos de verificación de identidad han dependido de contraseñas, tokens o documentos físicos de identidad, los cuales, aunque útiles, presentan múltiples vulnerabilidades (Al-Rajeh y Al-Shargabi, 2023). Las contraseñas, por ejemplo, pueden ser olvidadas, robadas o interceptadas, mientras que los documentos físicos son susceptibles a la falsificación o el robo (Mane y Bhosale, 2023). Además, Ryu et al. (2023) argumentan que la dependencia de contraseñas aumenta el riesgo de seguridad, ya que muchos usuarios tienden a reutilizar credenciales en múltiples plataformas.

Ante estos desafíos, los sistemas biométricos representan una solución tecnológica avanzada que ofrece un nuevo paradigma en la verificación de identidad. La biometría se basa en el uso de características físicas y conductuales únicas de cada individuo, como las huellas dactilares, el reconocimiento facial, el escaneo de iris, la voz o incluso los patrones de escritura de una persona (Arman et al., 2024). A diferencia de los métodos tradicionales como las contraseñas o identificaciones físicas, estos rasgos son inherentemente personales y difíciles de replicar, lo que proporciona una capa adicional de seguridad (Khan y Aithal, 2022). Según la Organización Internacional de Normalización (ISO, 2018) y la Comisión Electrotécnica Internacional, las tecnologías biométricas son consideradas uno de los métodos más confiables para la verificación de identidad debido a su alta precisión en la identificación de personas basándose en características inmutables a lo largo del tiempo. La biometría no solo se utiliza en aplicaciones cotidianas como el desbloqueo de teléfonos móviles o el acceso a cuentas bancarias, sino que también ha sido adoptada en sectores como la seguridad aeroportuaria, los servicios financieros, el control fronterizo, la atención médica y la gestión gubernamental (Labayen et al., 2021). Su creciente popularidad puede atribuirse a su capacidad de equilibrar conveniencia y seguridad: permite a los usuarios autenticar su identidad de manera rápida, mientras reduce significativamente el riesgo de accesos no autorizados.

Sin embargo, a pesar de sus innegables ventajas, los sistemas biométricos presentan importantes limitaciones que deben ser abordadas para garantizar su eficacia a largo plazo. Un desafío clave es la variabilidad en las condiciones de captura de las características biométricas. Por ejemplo, en el caso del reconocimiento facial, factores como la iluminación, el ángulo de captura, y las expresiones faciales pueden afectar la precisión del sistema. De igual manera, la huella dactilar puede verse comprometida por cortes, humedad o desgaste en los dedos del usuario, mientras que el escaneo de iris puede enfrentar dificultades cuando los usuarios usan gafas o lentes de contacto. Estos factores pueden generar tanto falsos negativos (rechazo de una identidad legítima) como falsos positivos (aceptación de una identidad incorrecta), lo que compromete la confiabilidad del sistema (Ezichi et al., 2020; Ryu et al., 2023). Además de las limitaciones técnicas, existen preocupaciones éticas y de privacidad relacionadas con el uso de los datos biométricos. El almacenamiento y manejo de esta información personal plantea interrogantes sobre el posible abuso, mal manejo o hackeo de los datos sensibles. En varios casos, la recolección y procesamiento de datos biométricos ha generado controversias,

especialmente cuando los usuarios no son plenamente conscientes de cómo se utilizan sus datos o no se les ofrece una opción de participación voluntaria (Chuquisengo, 2006; Mane y Bhosale, 2023). En 2021, el Tribunal Europeo de Derechos Humanos destacó la importancia de salvaguardar los derechos de los individuos frente al uso masivo de tecnologías biométricas, subrayando la necesidad de regulaciones sólidas que garanticen un uso ético y seguro de estas tecnologías (Défenseur des Droits, 2021; European Parliament, 2021a; European Parliament, 2021b).

Por lo tanto, el objetivo del estudio fue examinar la eficacia y las limitaciones de los sistemas biométricos en la verificación de identidad, considerando tanto sus beneficios como sus desafíos, además de las implicaciones éticas y de privacidad asociadas.

2. Metodología

Se utilizó la metodología PRISMA. De acuerdo a Page et al. (2021) esta metodología fue actualizada en 2020 y es esencial para garantizar la transparencia, calidad y reproducibilidad en revisiones sistemáticas y meta-análisis. Este conjunto de directrices ofrece un marco detallado para estructurar la recopilación, evaluación y presentación de estudios, reduciendo el sesgo de publicación y permitiendo una exposición exhaustiva de la evidencia recopilada. Asimismo, facilita la evaluación de la calidad y validez de los estudios incluidos, promueve la integridad científica y fortalece la confianza en los resultados. Finalmente, establece un estándar para la presentación clara y estructurada de revisiones sistemáticas, mejorando la interpretación de la evidencia y posibilitando la replicación de los hallazgos por otros investigadores.

Los datos fueron recolectados entre los meses de 15 de junio y 5 de julio de 2024, a partir de búsquedas en cuatro bases de datos académicas: Scopus, ScienceDirect, Google Académico y SpringerLink, utilizando palabras clave como "biometría", "verificación de identidad" y "sistemas biométricos" tal como se presenta en la Tabla 1.

Tabla 1

Ecuaciones de búsqueda de diferentes bases de datos

Base de dato	Ecuaciones de búsqueda
Scopus	Title-abs-key ((" biometric systems " OR " biometric technologies") AND ("identity verification" OR "identity authentication") AND ("efficacy" OR "effectiveness" OR "performance") AND ("limitations" OR "challenges" OR "constraints"))
ScienceDirect	Title("biometric systems" OR "biometric technologies") AND Title("identity verification" OR "identity authentication") AND Title("efficacy" OR "effectiveness" OR "performance") AND Title("limitations" OR "challenges")
Google Académico	Intitle:"biometric systems" AND "identity verification" AND (limitations OR challenges)
SpringerLink	Title("biometric systems" OR "biometric technologies") AND Title("identity verification" OR "identity authentication") AND Title("efficacy" OR "effectiveness" OR "performance") AND Title("limitations" OR "challenges")

Una vez recopilados los documentos de diversas bases de datos académicas, se procedió a aplicar un proceso de filtración basado en criterios de exclusión específicos, que fueron codificados como CE1 a CE6. Estos criterios, los cuales se describen en la Tabla 2, permitieron asegurar que solo se incluyeran aquellos artículos pertinentes para la revisión.

Tabla 2
Criterios de exclusión

Código	Descripción
CE1	Resultados que no son artículos originales o artículos de revisión.
CE2	Artículos publicados antes del año 2020.
CE3	Artículos que no están redactados en inglés o español.
CE4	Artículos a los cuales no se puede acceder.
CE5	Artículos que no se relacionan con la temática de la investigación.
CE6	Artículos que no han sido citados por otros autores.

Las ecuaciones de búsqueda formuladas en cada base de datos (Tabla 1) arrojaron un total de 277 resultados. Sin embargo, para garantizar que solo se consideraran fuentes de alta calidad y relevancia, se establecieron criterios de exclusión adicionales, los cuales se detallan en la Tabla 3. Estos criterios fueron fundamentales para el proceso de selección, ya que ayudaron a eliminar artículos que no cumplían con las condiciones necesarias para el análisis. Adicionalmente, en la Figura 1 se presenta diagrama de flujo PRISMA, el cual describe visualmente el proceso de selección de los documentos, desde la identificación de los registros hasta la inclusión de los artículos finales, junto con las razones de exclusión correspondientes.

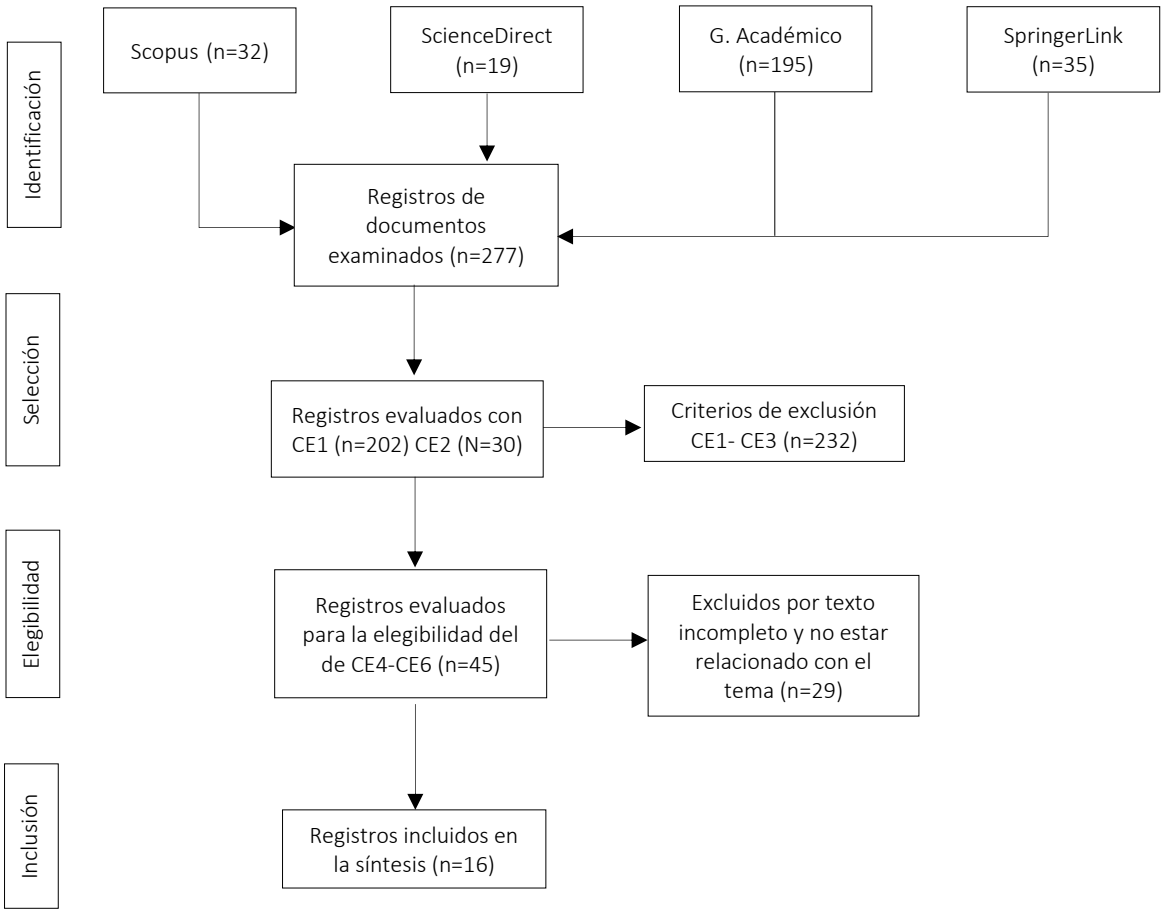
Tabla 3
Procedimiento de exclusión al aplicar los criterios de exclusión

Fuente	Resultados	CE1	CE2	CE3	CE4	CE5	CE6	Final
Scopus	32	17	7	0	3	1	0	4
ScienceDirect	19	4	4	0	6	4	0	1
Google Académico	191	158	16	0	4	1	3	9
SpringerLink	35	23	3	0	3	1	3	2

Por otra parte, El análisis bibliométrico se llevó a cabo utilizando Bibliometrix, un software basado en R que incluye la interfaz gráfica Biblioshiny. Esta herramienta destaca por su capacidad para realizar estudios detallados, como el mapeo de co-ocurrencia de palabras clave y países, la co-citación de revistas y el seguimiento de la evolución de temas de investigación. Su diseño combina métodos analíticos avanzados con una interfaz interactiva que facilita tanto la exploración de datos como la creación de visualizaciones dinámicas. Además, ofrece la opción de personalizar los análisis mediante scripts en R, adaptándose a las necesidades específicas de cada estudio (Aria y Cuccurullo, 2017).

Figura 1

Secuencia metodológica mediante el diagrama de flujo PRISMA



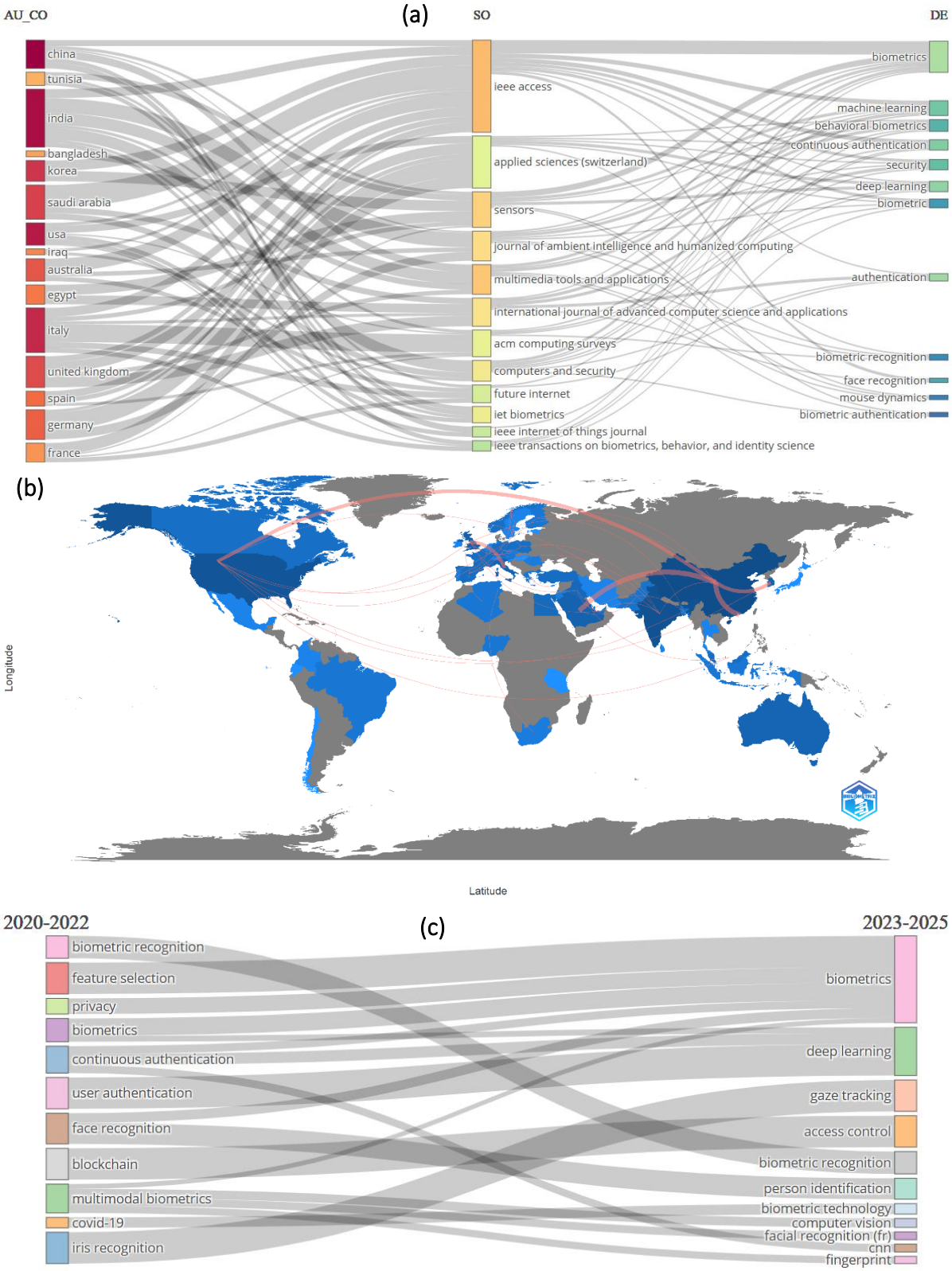
3. Resultados

3.1. Análisis bibliométrico

La Figura 2a muestra las conexiones entre los países de los autores (AU_CO), las revistas donde publicaron (SO) y los principales temas de estudio (DE). China, India y Estados Unidos destacan como los principales contribuyentes en investigación biométrica, lo que refleja su liderazgo tecnológico en este ámbito. Las revistas más influyentes, como *IEEE Access*, *Applied Sciences (Switzerland)* y *Sensors*, evidencian que la investigación en biometría se publica predominantemente en plataformas relacionadas con tecnología y aplicaciones científicas. Los temas dominantes, como "biometría", "aprendizaje profundo" y "autenticación continua", reflejan el interés creciente en mejorar técnicas de reconocimiento y fortalecer la seguridad, alineándose directamente con los objetivos de sistemas más eficaces. Mientras que la Figura 2b ilustra la interacción entre regiones. Destacan las colaboraciones activas entre Estados Unidos, Europa y Asia, en particular entre países como China, India y Alemania, lo que reafirma el papel de estos centros como motores globales de innovación. Sin embargo, la limitada participación de regiones como África y América Latina revela desigualdades significativas en términos de acceso a recursos y desarrollo de infraestructura tecnológica. Esto no solo evidencia las fortalezas colaborativas, sino también las brechas que podrían abordarse.

Figura 2

Cantidad de artículos encontrados por países



Nota. Las gráficas fueron creadas con el software bibliometrix, donde (a) representa al gráfico de tres campos, (b) el mapa mundial de colaboración entre países y (c) la evolución temática.

En esa línea, La Figura 2c, analiza la evolución temática entre 2020-2022 y 2023-2025, donde se evidencia una transición hacia tópicos más avanzados y específicos. Temas como "reconocimiento facial", "autenticación continua" y "blockchain", centrales en el periodo inicial, han dado paso a conceptos emergentes como "aprendizaje profundo", "rastreo ocular" y "control de acceso". Al mismo tiempo, se mantienen constantes palabras clave como "biometría" y "reconocimiento biométrico", destacando su relevancia transversal en el campo. El surgimiento de términos como "CNN"(Red Neuronal Convolucional) y "visión por computadora" subraya un enfoque en algoritmos más sofisticados para mejorar la precisión y la eficiencia.

3.2. Revisión sistemática

Una vez analizados los artículos seleccionados para la revisión, se procedió a recopilar los datos más relevantes, los cuales se sintetizan en la Tabla 4 que se muestra a continuación.

Tabla 4

Registros de los artículos analizados

N°	Autor/Año/Aporte	Factores que determinan la eficacia	Principales limitaciones
1	Arman et al. (2024) clasifican métodos de autenticación biométrica centrados en la privacidad, analizando desafíos y riesgos asociados. Sugieren estrategias para mitigar problemas y anticipan tendencias futuras en seguridad, autenticación y criptografía biométrica.	- Niveles de seguridad. - Desempeño. - Facilidad de uso. - Aplicaciones. - Compatibilidad con mecanismos de protección.	- Vulnerabilidad a ataques. - Complejidad en la implementación. - Problemas de exactitud. - Cuestiones de privacidad. - Costo y recursos.
2	Khan y Aithal (2022) revisan y comparan los sistemas de biometría de voz para la identificación y autenticación de usuarios, destacando las tecnologías más avanzadas y sus aplicaciones en sectores como la banca, seguridad informática y control de acceso. Además, explora las mejoras recientes en redes neuronales que han incrementado la eficacia de los sistemas biométricos de voz.	- La calidad del modelo. - El procesamiento adecuado de las señales de voz en sus fases de entrenamiento y prueba. - La tecnología de red neuronal aplicada al reconocimiento y autenticación.	- Dificultad para distinguir entre voces masculinas y femeninas en algunos sistemas. - Sensibilidad a las condiciones de salud del usuario que puedan afectar su voz. - Complejidad de implementación en sistemas IoT y la coordinación entre proveedores y usuarios.

Tabla 4 (Continuación/1)

N°	Autor/Año/Aporte	Factores que determinan la eficacia	Principales limitaciones
3	Labayen et al. (2021) presentaron un sistema de autenticación biométrica y supervisión continua para estudiantes impacto positivamente en la solución técnica, Mejora de la integridad académica y aceptación estudiantil y docente.	- Precisión del reconocimiento biométrico. - Condiciones ambientales. - Integración con LMS. - Escalabilidad y seguridad.	- Preocupaciones de privacidad. - Variabilidad en el rendimiento. - Dependencia de la tecnología. - Necesidad de verificación humana.
4	Khan y Efthymiou (2021), contribuyen a la literatura sobre biometría en entornos aeroportuarios, ofrecen un análisis detallado de las tecnologías de reconocimiento facial.	- Calidad de imágenes. - Condiciones de Iluminación. - Diversidad de nacionalidad y rango de edad de los usuarios. - Fiabilidad de la red. - Infraestructura del sistema.	- Baja tasa de coincidencia biométrica. - Problemas de conectividad. - Dependencia de cooperación de las empresas.
5	Tucci et al., (2024) presentaron una revisión sobre la aplicación de métodos de Inteligencia Artificial Explicable (XAI) en sistemas biométricos, destacando tendencias en metodologías y evaluación, y enfatizando la importancia de seguir directrices de diseño de HCI y de integrar métricas personalizadas para mejorar la confianza del usuario.	- Calidad de datos biométricos. - Robustez del modelo. - Diseño de explicaciones. - Cumplimiento de normativas.	- Falta de explicabilidad. - Sesgo de datos. - Limitaciones en el diseño de explicaciones. - Contexto de uso.
6	Dargan y Munish (2020) aportaron en la identificación de tendencias significativas en la evolución de la identidad digital, destacando el cambio hacia un paradigma centrado en el usuario. Además, el artículo resalta la creciente importancia de términos relacionados con biometría y blockchain.	- Calidad de datos biométricos. - Algoritmo de reconocimiento. - Entorno de capturas. - Tasa de error. - Interacción del usuario.	- Accesibilidad. - Falsas aceptaciones y rechazos.

Tabla 4 (Continuación/2)

N°	Autor/Año/Aporte	Factores que determinan la eficacia	Principales limitaciones
7	Genser et al. (2020) aportaron un diseño innovador de sensor de cámara en array y un enfoque para el emparejamiento estéreo multimodal en imágenes multiespectrales para identificación biométrica. También presentaron un método de calibración y una revisión de técnicas actuales, resaltando sus aplicaciones y limitaciones.	- Calidad de captura de imágenes. - Características biométricas únicas. - Algoritmos de reconocimiento. - Condiciones ambientales. - Capacidad de adaptación.	- Falsos aceptaciones y rechazos. - Costos. - Privacidad y ética. - Limitaciones técnicas. - Dependencia de condiciones.
8	Comb y Martin (2024) aportan al campo de la identidad digital destacando en identificación de tendencias, metodologías efectivas, Implicaciones para la innovación	- Calidad de datos biométricos. - Tecnología utilizada. - Adaptabilidad de diferentes condiciones. - Seguridad y protección de datos. - Usabilidad y experiencia del usuario.	- Problemas de privacidad. - Tasa de falsos aceptados y falsos rechazados. - Costo de implementación. - Dependencia de la tecnología.
9	Ezichi et al. (2020) contribuyen al campo de la seguridad biométrica al revisar dos estrategias de fusión a nivel de puntajes para sistemas multibiométricos: la regla de suma y la razón de verosimilitud. Presentan una comparación detallada entre ambas, analizando sus fortalezas, debilidades y aplicaciones más adecuadas, lo que ayuda a mejorar el rendimiento de los sistemas multibiométricos al seleccionar la estrategia de fusión más óptima.	- Calidad de las muestras biométricas. - La precisión del comparador (matcher).	- Dificultad de implementación en fusión temprana. - Necesidad de normalización de puntajes. - Complejidad y costo en sistemas basados en la razón de verosimilitud.

Tabla 4 (Continuación/3)

N°	Autor/Año/Aporte	Factores que determinan la eficacia	Principales limitaciones
10	Sharma y Dwivedi (2024) ofrecen una revisión sobre los avances en los sistemas de autenticación biométrica, incluyendo la evolución hacia sistemas multimodales y el uso de patrones de venas. Se destaca cómo estas nuevas tecnologías mejoran la seguridad, precisión y resistencia contra ataques de suplantación, especialmente con el uso de imágenes 3D y algoritmos de aprendizaje profundo (out).	- Calidad de los dispositivos de captura de datos biométricos. - Implementación de algoritmos avanzados, como redes neuronales profundas. - Uso de múltiples modalidades biométricas (multimodal) que combinan características fisiológicas y de comportamiento(out).	- Vulnerabilidad a ataques, como el uso de fotografías o muestras capturadas de usuarios. - Sensibilidad a variaciones externas, como la iluminación o la postura, en el caso de la biometría facial. - Costos elevados asociados a la implementación de dispositivos avanzados para la captura de imágenes de alta calidad(out).
11	Ryu et al. (2023) contribuyen al campo de la autenticación biométrica adaptativa al revisar de manera sistemática las modalidades y métricas de evaluación utilizadas, destacando la importancia de la usabilidad, escalabilidad y seguridad en el diseño de estos sistemas.	- Precisión de medición. - Usabilidad. - Escalabilidad. - Robustez frente a ataques.	- Falta de estandarización. - Dependencia de la calidad de los datos. - Problemas de privacidad y seguridad. - Costo y complejidad de implementación.
12	Sumalath et al. (2024) aportaron una revisión de los sistemas de autenticación biométrica de huellas dactilares, resaltando las diferencias entre enfoques unimodales y multimodales, y subrayando la importancia de la fusión de datos, protección de plantillas y la mitigación de ataques para mejorar la seguridad y efectividad de estos sistemas.	- Precisión y exactitud. - No universalidad. - Variaciones en clase. - Escalabilidad.	- Vulnerabilidad de ataques de suplantación. - Invariabilidad y ruido en los datos. - Privacidad. - Desafíos de escalabilidad.

Tabla 4 (Continuación/4)

N°	Autor/Año/Aporte	Factores que determinan la eficacia	Principales limitaciones
13	El-Dahshan et al. (2021) presentan una revisión de las tecnologías y metodologías utilizadas en los sistemas biométricos de fonocardiograma (PCG), abarcando diferentes fases del proceso desde la adquisición de datos hasta la evaluación	- Calidad de la adquisición de datos. - Preprocesamiento de señales. - Extracción de características. - Tamaño y diversidad del conjunto de datos.	- Variabilidad de señales. - Ruido y artefactos. - Limitaciones de los dispositivos. - Falta de estándares. - Escalabilidad y costos.
14	Mane y Bhosale (2023) destacan cómo los sistemas biométricos multimodales y basados en patrones de venas mejoran la seguridad y precisión en la autenticación de usuarios, utilizando técnicas avanzadas como la fusión de múltiples rasgos biométricos y aprendizaje profundo.	- Calidad de la captura de datos. - Métodos de fusión biométrica. - Algoritmos de extracción. - Liveness detección - Adaptación a factores externos.	- Vulnerabilidad a ataques de falsificación. - Privacidad y seguridad. - Errores de autenticación. - Factores externos.
15	Albalawi et al. (2022) establecen criterios para evaluar técnicas de reconocimiento biométrico, destacando la propuesta de un sistema de identificación por iris que utiliza PCA y SVM, mejorando así la precisión en contextos críticos. Se enfatiza la importancia de la segmentación del iris y la calidad de la imagen en la eficacia del sistema.	- Precisión. - Uso de algoritmos avanzados. - Resistencia a variaciones.	- Calidad de la imagen. - Desafíos en la segmentación. - Costo y accesibilidad. - Condiciones ambientales. - Preocupaciones de privacidad.
16	Al-Rajeh y Al-Shargabi (2023) analizan técnicas de detección de ataques de presentación en sistemas biométricos de iris, abordando la seguridad en la verificación de identidad. También destacan estrategias de ataque y proponen direcciones futuras para mejorar la eficacia de estos sistemas.	- Calidad de imágenes. - Verificación de tejido vivo. - Robustez en entornos no controlados. - Técnicas de detección de ataques.	- Susceptibilidad de ataques de presentación. - Dificultades en condiciones no controladas. - Sesgos en el rendimiento. - Complejidad de los algoritmos.

4. Discusión

La efectividad y las limitaciones de los sistemas biométricos son temas recurrentes en la literatura actual, lo que enfatiza la necesidad de considerar estos aspectos en el desarrollo e implementación de tecnologías de autenticación. En su investigación, Shanhriar et al. (2024) subrayan la importancia de encontrar un equilibrio entre la seguridad y la privacidad en los sistemas biométricos, indicando que tanto los niveles de seguridad como la facilidad de uso son elementos fundamentales para su eficacia. Sin embargo, también advierten sobre la vulnerabilidad a ataques y las complejidades en su implementación, que representan limitaciones significativas a tener en cuenta. Por otra parte, Nils et al. (2020) presentan un enfoque novedoso utilizando sensores de cámara en array y métodos de emparejamiento multimodal, poniendo de relieve la relevancia de la calidad de la captura de imágenes y las condiciones ambientales en la precisión del reconocimiento biométrico. No obstante, su dependencia de circunstancias específicas y las inquietudes relacionadas con la privacidad generan preocupaciones serias sobre su viabilidad práctica.

En cuanto a la seguridad, Noura y Amal (2023) se enfoca en la detección de ataques de presentación en sistemas biométricos de iris, reflejando así una creciente preocupación por la seguridad en la verificación de identidad. A pesar de sus aportes en términos de robustez y calidad de imagen, la vulnerabilidad a ataques y los desafíos en entornos no controlados destacan la complejidad de asegurar un sistema biométrico confiable. En un enfoque más aplicado, Mikel et al. (2021) introducen un sistema de autenticación biométrica para estudiantes, que pone énfasis en la importancia de integrar estas tecnologías con plataformas de gestión de aprendizaje (LMS) y en su escalabilidad. Sin embargo, las inquietudes sobre la privacidad y la necesidad de verificación humana sugieren que, aunque estas tecnologías podrían mejorar la integridad académica, su aceptación podría estar restringida por las percepciones de los usuarios en relación a la privacidad. Tucci et al. (2024) aportan una perspectiva centrada en el usuario al explorar la Inteligencia Artificial Explicable (XAI) en sistemas biométricos, sugiriendo que la falta de explicabilidad y los sesgos en los datos pueden tener un impacto negativo en la confianza del usuario. Esto se complementa con los hallazgos de Comb y Martin (2024), quienes examinan la usabilidad y seguridad en la identidad digital, enfatizando la necesidad de adaptar las tecnologías a diferentes contextos y requerimientos de los usuarios.

Desde un enfoque técnico, Ryu et al. (2023) analizan la autenticación biométrica adaptativa, poniendo de relieve su escalabilidad y usabilidad, mientras que Sumalat et al. (2024) abordan la efectividad de los sistemas de huellas dactilares, subrayando que la fusión de datos y la mitigación de ataques son vitales para mejorar la seguridad. Estos estudios ponen de manifiesto que, a pesar de la evolución de las tecnologías biométricas, aún existen desafíos relacionados con su vulnerabilidad y complejidad. Por último, los trabajos de Dahshan y Bassiouni (2021) sobre tecnologías de fonocardiograma y de Khan y Aithal (2022) sobre biometría de voz ilustran la diversidad de aplicaciones biométricas. Sin embargo, estas investigaciones también coinciden en señalar la necesidad de establecer estándares claros y superar las complejidades asociadas con su implementación. En conjunto, estos hallazgos refuerzan la importancia de enfoques sistemáticos e integrales que aborden tanto las fortalezas como las limitaciones inherentes a los sistemas biométricos para garantizar su eficacia y aceptación en un mundo en constante evolución.

5. Conclusiones

Los sistemas biométricos representan una solución innovadora para la autenticación y verificación de identidad, con importantes ventajas en seguridad y eficiencia. Sin embargo, su eficacia depende de factores como la calidad de los datos biométricos, la precisión del reconocimiento, la facilidad de uso y su integración con otras plataformas. Asimismo, la adaptabilidad a diversas condiciones y un diseño centrado en el usuario resultan esenciales para optimizar su desempeño y fomentar su aceptación. A pesar de sus beneficios, estas tecnologías enfrentan desafíos importantes. Las preocupaciones sobre la privacidad, la vulnerabilidad ante ataques de suplantación y la complejidad técnica de su implementación plantean obstáculos significativos. Además, su rendimiento puede verse limitado en entornos no controlados debido a su dependencia de condiciones específicas. Superar estas limitaciones es clave para fortalecer la confianza del usuario y asegurar su aplicación efectiva.

6. Referencias Bibliográficas

Albalawi, S., Alshahrani, L., Albalawi, N., Kilabi, R., y Alhakamy, A. (2022). A comprehensive overview on biometric authentication systems using artificial intelligence techniques. *International Journal of Advanced Computer Science and Applications : IJACSA*, *13*(4). https://doi.org/10.14569/ijacsa.2022.0130491

Al-Rajeh, N. S., y Al-Shargabi, A. A. (2023). Iris presentation attack detection: Research trends, challenges, and future directions. *Journal of Autonomous Intelligence*, *7*(2). https://doi.org/10.32629/jai.v7i2.1012

Aria, M., y Cuccurullo, C. (2017). bibliometrix: An R-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959–975. https://doi.org/10.1016/j.joi.2017.08.007

Arman, S. M., Yang, T., Shahed, S., Mazroa, A. A., Attiah, A., y Mohaisen, L. (2024). A comprehensive survey for privacy-preserving biometrics: Recent approaches, challenges, and future directions. *Computers, Materials & Continua*, *78*(2), 2087–2110. https://doi.org/10.32604/cmc.2024.047870

Comb, M., y Martin, A. (2024). Mining digital identity insights: patent analysis using NLP. *EURASIP Journal on Information Security*, *2024*(1). https://doi.org/10.1186/s13635-024-00172-5

Défenseur des Droits (2021). *Biometrics: the urge to safeguard fundamental rights*. https://www.defenseurdesdroits.fr/sites/default/files/2023-07/ddd_rapport_technologies-biometriques_2021_EN.pdf

El-Dahshan, E.-S. A., Bassiouni, M. M., Sharvia, S., y Salem, A.-B. M. (2021). PCG signals for biometric authentication systems: An in-depth review. *Computer Science Review*, *41*(100420), 100420. https://doi.org/10.1016/j.cosrev.2021.100420

European Parliament. (2021a). *Biometric Recognition and Behavioural Detection: Assessing the ethical aspects of biometric recognition and behavioural detection techniques with a focus on their current and future use in public spaces.*

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf

European Parliament. (2021b). *Person identification, human rights and ethical principles: Rethinking biometrics in the era of artificial intelligence.* https://www.europarl.europa.eu/regdata/etudes/stud/2021/697191/eprs_stu(2021)697191_en.pdf

Ezichi, S. I., Ezika, I. J. F., Nkpume, C., y Iloanusi, O. N. (2020). Biometric security: A review of the sum rule and the likelihood ratio fusion algorithms for multibiometric systems [Conferencia]. *2020 LGT-ECE-UNN International Conference: Technological Innovation for Holistic Sustainable Development*, Nsukka, Nigeria https://www.researchgate.net/publication/351461712_Biometric_Security_A_Review_of_the_Sum_Rule_and_the_Likelihood_Ratio_Fusion_Algorithms_for_Multibiometric_Systems

Genser, N., Seiler, J., y Kaup, A. (2020). Camera array for multi-spectral imaging. *IEEE transactions on image processing: a publication of the IEEE Signal Processing Society*, *29*, 9234–9249. https://doi.org/10.1109/tip.2020.3024738

Ghadge, M. N. (2024). Digital identity in the age of cybersecurity: Challenges and solutions. *Global Journal of Computer Science and Technology*, 1–9. https://doi.org/10.34257/ljrcstvol24is1pg1

International Organization for Standardization (ISO). (2018). *Information technology — Biometrics — Overview and application.* https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:24741:ed-2:v1:en

Khan, A. H., y Aithal, P. S. (2022). Voice biometric systems for user identification and authentication – A literature review. *International Journal of Applied Engineering and Management Letters*, 198–209. https://doi.org/10.47992/ijaeml.2581.7000.0131

Khan, N., y Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). *International Journal of Information Management Data Insights*, *1*(2), 100049. https://doi.org/10.1016/j.jjimei.2021.100049

Labayen, M., Vea, R., Florez, J., Aginako, N., y Sierra, B. (2021). Online student authentication and proctoring system based on multimodal biometrics technology. *IEEE access: practical innovations, open solutions*, *9*, 72398–72411. https://doi.org/10.1109/access.2021.3079375

Mane, J. S., y Bhosale, S. (2023). Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. *Revue d intelligence artificielle*, *37*(3), 709–718. https://doi.org/10.18280/ria.370319

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., mayo-Wilson, E., McDonald, S., … Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ (Clinical Research Ed.)*, n71. https://doi.org/10.1136/bmj.n71

Ryu, R., Yeom, S., Herbert, D., y Dermoudy, J. (2023). The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express*, *9*(6), 1183–1197. https://doi.org/10.1016/j.icte.2023.04.003

Serratosa, F. (2020). Security in biometric systems. En *arXiv [cs.CR]*. https://doi.org/10.48550/ARXIV.2011.05679

Sharma, S., y Dwivedi, R. (2024). A survey on blockchain deployment for biometric systems. *IET Blockchain*, *4*(2), 124–151. https://doi.org/10.1049/blc2.12063

Shaveta, D., y Munish, K. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications*, *143*(113114), 113114. https://doi.org/10.1016/j.eswa.2019.113114

Sumalatha, U., Prakasha, K. K., Prabhu, S., y Nayak, V. C. (2024). A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. *IEEE access: practical innovations, open solutions*, *12*, 64300–64334. https://doi.org/10.1109/access.2024.3395417

Tucci, C., Della Greca, A., Tortora, G., y Francese, R. (2024). Explainable biometrics: a systematic literature review. *Journal of Ambient Intelligence and Humanized Computing*. https://doi.org/10.1007/s12652-024-04856-1