INGENIERÍA INVESTIGA

Vol. 5, e866, año 2023
ISSN – Online: 2708-3039
DOI: https://doi.org/10.47796/ing.v5i0.866

Artículo de revisión

La vulnerabilidad de las tecnologías biométricas en la autenticación

The Vulnerability of Biometric Technologies in Authentication

Jair Joel Vásquez Cerna[1]
https://orcid.org/0000-0002-6182-5554

Luz Maria Solano Quincho[2]
https://orcid.org/0009-0002-2243-7388

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

Recibido: 4/10/2023
Aceptado: 15/12/2023
Publicado: 28/12/2023

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

E-mail: [1]to53300420@unitru.edu.pe, [2]to23300520@unitru.edu.pe, [3]amendozad@unitru.edu.pe

Facultad de Ingeniería
Publicación Oficial

Resumen

El avance tecnológico y la creciente necesidad de proteger datos sensibles han incrementado la importancia de la biometría en el ámbito de la seguridad. Su aplicación se ha extendido a dispositivos móviles y la gestión de identidades, pero a medida que se integra en la vida cotidiana y en el entorno empresarial, surgen desafíos en términos de privacidad y seguridad. Por lo tanto, es fundamental evaluar las posibles vulnerabilidades en la autenticación biométrica. Para llevar a cabo esta evaluación, se analizaron documentos almacenados en diversas bases de datos, incluyendo IEEE Xplore, SciELO, ScienceDirect y Scopus. Se aplicaron criterios de inclusión y exclusión, lo que permitió la selección de 20 artículos. Los hallazgos identificaron varias amenazas, como la reconstrucción de huellas dactilares y ataques de presentación, así como soluciones propuestas, como representaciones en 3D y sistemas de verificación. Además, se resalta la necesidad de contar con tecnologías de detección de ataques y regulaciones éticas. Por último, se enfatiza la importancia de garantizar la seguridad y la privacidad en los sistemas de autenticación biométrica, lo que impulsa la investigación constante para mantenerse alineadas con las amenazas en constante evolución.

Palabras clave: autenticación; seguridad digital; tecnologías biométricas; vulnerabilidades.

Abstract

Technological advancements and the increasing necessity to protect sensitive data have elevated the significance of biometrics in the realm of security. Its application has expanded to encompass mobile devices and identity management. Nevertheless, as it integrates into everyday life and the business environment, challenges concerning privacy and security surface inevitably. Therefore, it is imperative to evaluate potential vulnerabilities in biometric authentication. For the purpose of this evaluation, documents stored in various databases, including IEEE Xplore, SciELO, ScienceDirect, and Scopus, were analyzed. Inclusion and exclusion criteria were applied, allowing the selection of 20 articles. The findings uncovered several threats, such as fingerprint reconstruction and presentation attacks, along with proposed solutions like 3D representations and verification systems. Furthermore, it underscores the necessity for advanced attack detection technologies and ethical regulations. In conclusion, it emphasizes the paramount importance of ensuring security and privacy in biometric authentication systems, driving continuous research efforts to remain in step with ever-evolving threats.

Keywords: authentication; digital security; biometric technologies; vulnerabilities.

1. Introducción

La biometría abarca el reconocimiento automático de individuos a través de características únicas del cuerpo o el comportamiento humano (Jain et al., 2022). Esta disciplina fascinante deriva su nombre de las raíces griegas *"bios"* (vida) y *"metron"* (medida), resaltando la importancia de medir atributos esenciales para la identificación de personas. Entre los atributos más comunes en la biometría se encuentran el rostro, las huellas dactilares y el iris. En particular, la biometría moderna ha popularizado el uso de atributos de voz y rostro debido a su facilidad de adquisición y aplicabilidad en diversas situaciones cotidianas (Mandalapu et al., 2021).

Por otro lado, el mundo digital en constante evolución presenta desafíos continuos en la autenticación de usuarios y el acceso seguro a la información. Actualmente, los métodos tradicionales de autenticación, como los PIN y las contraseñas, han sido complementados por avances significativos en tecnologías biométricas, como el reconocimiento facial, de huellas dactilares y del iris (Baig et al., 2023). Las técnicas actuales son efectivas al iniciar sesiones, pero la autenticación futura apunta a ser más sofisticada y cómoda, con la autenticación continua y adaptativa. Esto garantiza la seguridad en la era digital, donde las amenazas cibernéticas son omnipresentes y avanzadas.

Sin embargo, las tecnologías biométricas, a pesar de su eficacia, no están exentas de vulnerabilidades. En este sentido, Morales et al. (2021) describen una de las vulnerabilidades más destacadas relacionadas con la presentación de PAIs (Impostor Artificialmente Presentado), como fotografías o videos que imitan las características de los iris reales. Esto destaca la importancia de contar con sistemas de autenticación biométrica robustos.

Por otra parte, Sarkar et al. (2022) indican que los sistemas de reconocimiento facial basados en redes neuronales, como VGG-Face, ArcFace y FaceNet, son vulnerables a los ataques de Morphing, en los que se combinan imágenes faciales para engañar a los sistemas de reconocimiento facial. Estos ataques plantean desafíos significativos para la seguridad biométrica, resaltando la necesidad de implementar medidas sólidas de detección de ataques. Además, Mandalapu et al. (2021) destacan la vulnerabilidad de la biometría audiovisual a ataques de presentación, donde se usan muestras falsificadas como grabaciones de voz o imágenes faciales para acceder ilegítimamente. La importancia de la detección de ataques de presentación (PAD) es crucial para mitigar esta amenaza en la autenticación biométrica, enfatizando la necesidad de abordar las vulnerabilidades de manera efectiva y proactiva.

Por consiguiente, el objetivo del estudio fue analizar las vulnerabilidades vinculadas a las tecnologías biométricas en los procesos de autenticación. Para ello, se llevó a cabo una revisión sistemática de la literatura para identificar y comprender las amenazas más relevantes en este ámbito. Además, se exploran posibles soluciones y estrategias de mitigación destinadas a asegurar una autenticación segura en la era digital.

2. Metodología

Para investigar las vulnerabilidades en la autenticación a través de tecnologías biométricas, se realizó una revisión exhaustiva de la literatura mediante la metodología PRISMA. Este enfoque

se presenta como una estructura que simplifica la ejecución de una revisión sistemática sustentada en investigaciones previas (Page et al., 2021).

2.1. Criterios de inclusión y exclusión

Para la selección de los documentos, se aplicaron criterios de inclusión y exclusión para garantizar la relevancia y calidad de la información recopilada. Los criterios se detallan a continuación:

Los criterios de inclusión se basaron en la disponibilidad en línea de los documentos a través de bases de datos académicas o fuentes de investigación confiables. Además, se priorizaron investigaciones científicas, estudios técnicos, informes de seguridad y artículos académicos que proporcionaran un análisis sólido y fundamentado sobre el tema, en particular, durante los últimos cuatro años, desde 2019 hasta 2023.

En cuanto a los criterios de exclusión, se descartaron los documentos que no estaban relacionados con la vulnerabilidad de las tecnologías biométricas en la autenticación. Asimismo, se excluyeron aquellos documentos anteriores a 2019 o que no proporcionaban información actualizada, con el objetivo de centrarse en investigaciones contemporáneas.

2.2. Estrategia de búsqueda

Se aplicaron estrategias específicas para localizar información pertinente sobre el tema en cuestión. Estas estrategias se fundamentaron en la utilización de términos clave y la exploración de diversas fuentes de información. Los términos clave vinculados a "biometría," "vulnerabilidad," y "riesgo" se emplearon en diversas combinaciones con el propósito de ampliar la búsqueda y abordar diferentes facetas de la vulnerabilidad en la autenticación biométrica., como se muestra en la Tabla y Figura 1.

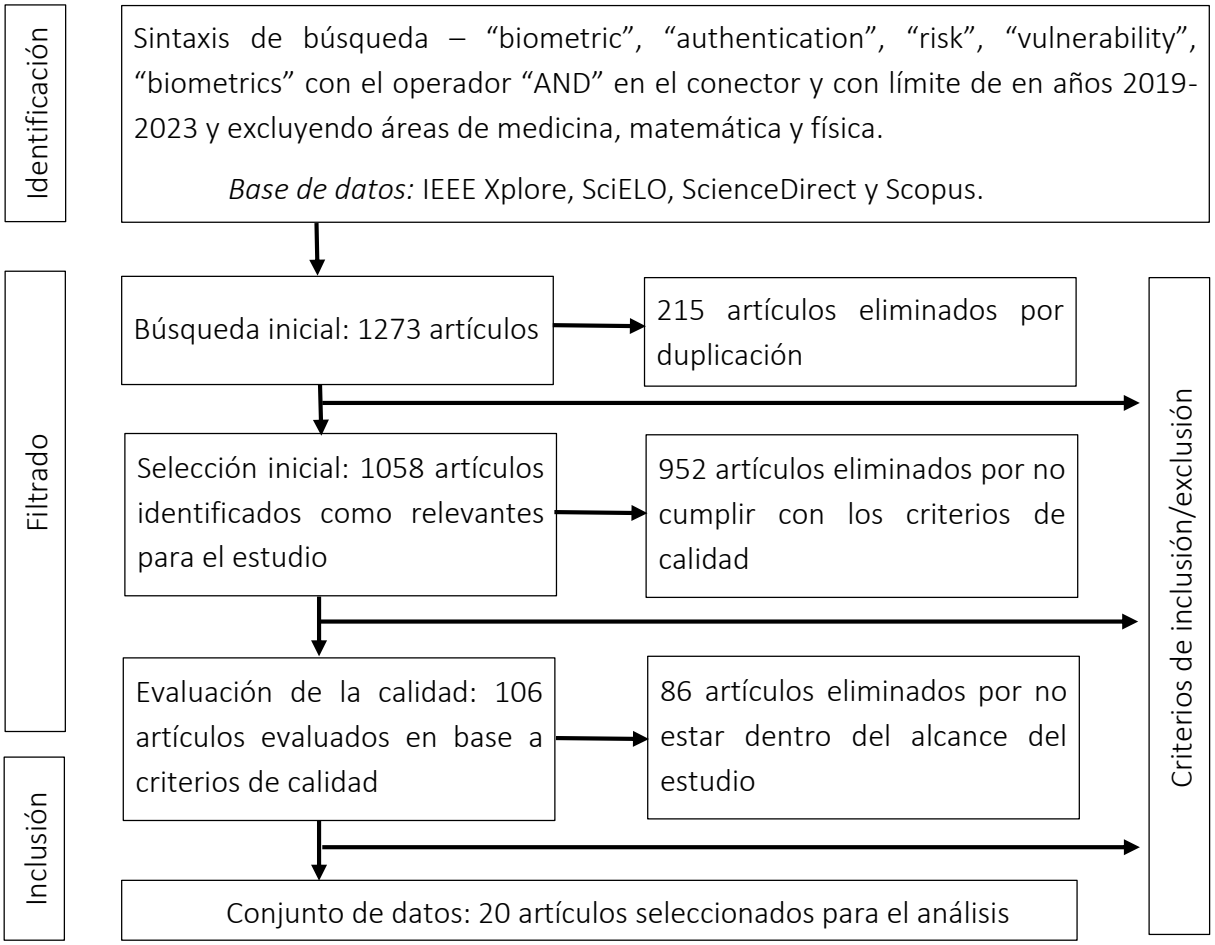
Tabla 1

Términos de búsqueda en base de datos

Base de datos	Términos de Búsqueda	Resultados	Seleccionados
EEE Xplore	(Document Title: Biometrics AND All Metadata: Risk); (Document Title: Biometrics AND All Metadata: Vulnerability); (Document Title: Biometric AND All Metadata: Risk); (Document Title: Biometric AND All Metadata: Vulnerability)	18	3
SciELO	biometric and authentication	6	1
ScienceDirect	(Title, abstract, keywords: risk AND Title: biometric); (Title, abstract, keywords: vulnerability AND Title: biometric); (Journal or book title: biometric AND Title, abstract, keywords: risk)	45	6
Scopus	(Title: biometric AND Title: risk); (Title: biometrics AND Title: risk); (Title: biometric AND Title: vulnerability); (Title: biometrics AND Title -Abs-Key: vulnerability)	37	10

Figura 1

Esquema de términos de búsqueda en base de datos



3. Resultados

En la Tabla 2, se presenta la literatura relacionada con la vulnerabilidad de las tecnologías biométricas en autenticación, habiéndose analizado un total de 20 artículos. Asimismo, se resalta una síntesis de los principales hallazgos identificados, junto con las soluciones y medidas de seguridad correspondientes para hacer frente a esta vulnerabilidad.

Tabla 2

Análisis de los artículos académicos

N°	Autores	Vulnerabilidad	Solución
1	Goh et al. (2022)	Reversibilidad de las plantillas biométricas.	Desarrollar algoritmos de reconstrucción biométrica, evaluar los riesgos asociados a estos algoritmos, implementar contramedidas para proteger las plantillas y seguir estándares como ISO/IEC 24745 para promover la irreversibilidad.

Tabla 2 (continuación/1)

2	Ali et al. (2020)	Uso de minutiae points directamente como plantilla de usuario, lo que puede llevar a la reconstrucción de la huella original.	Creación de representaciones en 3D de huellas dactilares mediante la generación de tripletes de minucias. Esto fortalece la seguridad al prevenir la reconstrucción de huellas originales y se refuerza aún más mediante el uso de claves únicas para cada usuario, lo que mejora la seguridad y la capacidad de revocación del sistema de autenticación biométrica.
3	Bera et al. (2021)	La exposición a ataques automatizados de bots en la autenticación de usuarios en redes sociales y otros servicios en línea.	Se propone un sistema de verificación en dos etapas que combina un CAPTCHA manual (HandCAPTCHA) con autenticación biométrica basada en imágenes reales de la mano con detección de ataques de presentación (PAD).
4	Schuiki et al. (2020)	Susceptibilidad a ataques de presentación en sistemas de reconocimiento de venas en la mano	Evaluación exhaustiva de amenazas utilizando diferentes esquemas de reconocimiento de venas para medir el potencial de los ataques de presentación. Uso de la fusión de puntuaciones de similitud generadas por múltiples esquemas de reconocimiento como una estrategia de detección de ataques de presentación.
5	Blanchard et al. (2020)	Vulnerables a ataques de reproducción y al robo irrevocable de credenciales, especialmente en el caso de biometrías basadas en el ojo.	Propone implementar un protocolo biométrico basado en la creación de memoria que combina elementos de la biometría ocular, sistemas de desafío y utiliza el "efecto de memoria de la pupila". Este protocolo ofrece un alto nivel de seguridad y la capacidad de revocar credenciales sin afectar al usuario, abordando así la vulnerabilidad de reproducción y robo irrevocable de credenciales.
6	Bernal-Romero et al. (2023)	Exposición de rasgos biométricos en la vida diaria.	Propone implementar técnicas cancelables en sistemas biométricos. Estas técnicas permiten la protección de la información biométrica al generar plantillas biométricas modificables y temporales.

Tabla 2 (continuación/2)

7	Bruno et al. (2021)	Spoofing de imágenes para engañar el análisis basado en PNU.	A pesar de que el spoofing puede parecer exitoso, el artículo destaca que las imágenes falsificadas aún conservan trazas de la cámara original. Estas trazas pueden ser utilizadas para mejorar la identificación de las imágenes falsificadas, lo que podría fortalecer la seguridad de las tecnologías biométricas basadas en el análisis de PNU.
8	De Abiega-L'Eglisse et al. (2022)	Vulnerabilidad a ataques de fuerza bruta en sistemas biométricos.	Uso de técnicas criptográficas avanzadas, incluyendo una función hash para generar un valor hash a partir del vault original, un mecanismo de encapsulación de clave para establecer una clave secreta criptográfica, y cifrado simétrico de los datos de unión que combina la clave secreta con los datos biométricos durante la etapa de inscripción.
9	Goicoechea-Telleria et al. (2019)	Ataques de Presentación en la Captura de Huellas Dactilares.	Uso de microscopios de bajo costo con iluminación especial para capturar imágenes de huellas dactilares. Además, se realizan evaluaciones exhaustivas de diferentes longitudes de onda y se aplica un filtro específico (610 nm) en el canal rojo de la imagen. Esto permite obtener tasas de error extremadamente bajas (1,78 % en la clasificación de ataques de presentación) y garantiza que el enfoque cumpla con los estándares de detección de ataques de presentación (ISO/IEC 30107-3).
10	Joshi et al. (2020)	Reconstrucción de huellas dactilares.	La solución propuesta implica el uso de técnicas avanzadas de cifrado para proteger las plantillas biométricas almacenadas, además, se implementan medidas de autenticación robustas para verificar la identidad del usuario antes de permitir el acceso a las plantillas biométricas, añadiendo una capa adicional de seguridad a los sistemas biométricos de huellas dactilares.

Tabla 2 (continuación/3)

11	Hernandez-Ortega et al. (2023)	Susceptibilidad a ataques de presentación. Estos ataques ocurren cuando un atacante presenta al sensor del sistema, generalmente una cámara, un Instrumento de Ataque de Presentación (PAI), que suele ser una fotografía, un video o una máscara, con el objetivo de intentar suplantar a un usuario legítimo.	Recomienda la implementación de técnicas de Detección de Ataques de Presentación (PAD) en sistemas de reconocimiento facial. Estas técnicas automatizan la detección de ataques de presentación, priorizando la detección de liveness para resistir PAIs como fotos impresas. Es esencial incorporar el PAD desde la fase inicial del sistema y seguir desarrollando nuevas técnicas para mantenerse actualizado ante amenazas emergentes.
12	Lee et al. (2021)	La autenticación basada en huellas digitales tiene vulnerabilidades, como la exposición de datos biométricos y la necesidad de hardware adicional, como escáneres de huellas digitales.	Se propone un modelo que combina la autenticación biométrica y conductual utilizando la longitud de la región de contacto entre tres dedos en una pantalla táctil y datos de sensores de aceleración en un reloj inteligente. Esto mejora la seguridad y comodidad en entornos con información confidencial.
13	Gomez-Barrero & Galbally (2020)	Reversibilidad de las plantillas biométricas	Desarrollar algoritmos de reconstrucción biométrica, evaluar los riesgos asociados a estos algoritmos, implementar contramedidas para proteger las plantillas y seguir estándares como ISO/IEC 24745 para promover la irreversibilidad.
14	Nakanishi & Maruoka (2019)	Vulnerable al robo de identidad, especialmente en sistemas de gestión de usuarios.	Se propone un enfoque de autenticación basado en ondas cerebrales (EEG) inducidas por ultrasonido. Este sistema utiliza estímulos de ultrasonido inaudibles para evocar respuestas en las ondas cerebrales de los usuarios y verifica la identidad utilizando características de EEG, como el espectro de potencia y características no lineales.

Tabla 2 (continuación/4)

15	Lee, Teoh et al. (2021)	Riesgo asociado a la pérdida del token	Un esquema de biométrica cancelable sin token llamado "Multimodal Extended Feature Vector (M·EFV) Hashing". Este enfoque elimina la necesidad de un token y utiliza un mecanismo de encriptación/desencriptación XOR para operar en la clave de transformación, reduciendo así el riesgo asociado a la pérdida del token.
16	Morales et al. (2021)	Uso de fotos y videos como Presentation Attacks, lo que permite a un atacante utilizar imágenes de alta resolución o videos para engañar a los sistemas de reconocimiento de iris.	Se propone la implementación de métodos de detección de ataques (PAD) que analicen la autenticidad de las muestras de iris mediante el estudio del movimiento, la textura y la profundidad. Además, se busca mejorar la calidad de las imágenes capturadas para prevenir la presentación de fotos y videos como auténticos.
17	Norstrom & Anekanta Consulting (2021)	Uso no regulado y generalizado de la tecnología de reconocimiento facial	Implementación de regulaciones claras y éticas que definan dónde y cómo se puede utilizar la tecnología, la realización de evaluaciones exhaustivas de impacto en la privacidad antes de su implementación, y la exigencia de autorizaciones por parte de autoridades competentes.
18	Tsitiridis et al. (2019)	La susceptibilidad de los sistemas de reconocimiento facial a los ataques de presentación, que incluyen intentos de engañar al sistema mediante el uso de imágenes impresas, pantallas digitales u otros métodos para falsificar una identidad	La solución propuesta es el desarrollo y la implementación de un modelo de detección de ataques de presentación denominado "BIOPAD". Este modelo se inspira en procesos biológicos que ocurren en el cerebro humano durante la percepción facial y utiliza características basadas en Gabor para identificar posibles ataques de presentación. El modelo BIOPAD se ha evaluado con éxito y ha demostrado tasas de detección de ataques muy altas, de hasta un 99 % de precisión en ciertos casos.

Tabla 2 (continuación/5)

19	Shukla et al. (2020)	Posibilidad de comprometer sistemas de autenticación EEG al explotar la correlación entre movimientos de la mano y señales cerebrales.	Evaluar de manera más rigurosa el rendimiento de los sistemas EEG para identificar vulnerabilidades. 2. Investigar y desarrollar tecnologías de defensa más efectivas contra ataques de falsificación basados en la correlación de datos biométricos. 3. Implementar una metodología de fusión avanzada que mejore la autenticación EEG y sea menos vulnerable a estos ataques.
20	Sobabe et al. (2020)	Intrinsic Failure (Fallo Intrínseco): Los sistemas biométricos pueden generar decisiones incorrectas debido a similitudes en los rasgos biométricos de diferentes usuarios.	Uso de meta data, como marcas y maquillaje, para distinguir entre individuos con rasgos biométricos similares, como gemelos idénticos. Integración de datos biométricos suaves (soft biometrics) para abordar variaciones intrausuario. Consideración de las características de volumen y brillo en la detección de rasgos biométricos.

4. Discusión

De los documentos analizados, se muestra una variedad de vulnerabilidades en las tecnologías biométricas utilizadas en procesos de autenticación, así como las soluciones propuestas por los investigadores para abordar estos desafíos. En primera línea, se encuentra la investigación de Ali et al. (2020), señalan la vulnerabilidad de la autenticación basada en huellas dactilares debido al uso de minutiae points como plantillas de usuario. La solución propuesta implica la creación de representaciones en 3D de huellas dactilares, lo que fortalece la seguridad al prevenir la reconstrucción de huellas originales.

Respecto a los ataques de presentación, los autores Bera et al. (2021) y Joshi et al. (2020), destacan la exposición a ataques de presentación en sistemas biométricos. Las soluciones incluyen la implementación de sistemas de verificación en dos etapas y la incorporación de medidas de autenticación robustas. Por otro lado, Morales et al. (2021) indican que la solución para la vulnerabilidad a la presentación del uso de fotos y videos en Presentation Attacks, involucran el uso de métodos de detección de ataques que analiza la autenticación de las muestras de iris.

Por otro lado, Shukla et al. (2020) proponen medidas para evaluar el rendimiento de los sistemas de vulnerabilidad de los sistemas de autenticación EEG y desarrollar tecnologías de defensa mas efectivas. Además, Sobabe et al. (2020) sugiere a integración de datos biométricos suaves y la consideración de características adicionales, como meta data para abordar la problemática del Intrinsic Failure. Por último, Blanchard et al. (2020) propone combinar elementos de la biometría ocular y sistemas de desafíos para solucionar los ataques de reproducción en este campo.

Además, se sugiere investigar la implementación de enfoques biométricos cancelables en combinación con técnicas de cifrado avanzadas, como se propone para abordar la vulnerabilidad a ataques de fuerza bruta (De Abiega-L'Eglisse et al., 2022). Esta combinación podría proporcionar una capa adicional de seguridad al proteger las plantillas biométricas de manera más efectiva durante la transmisión y el almacenamiento.

Como dirección futura, se sugiere llevar a cabo investigaciones más específicas en modalidades biométricas menos exploradas y en entornos particulares, como entornos móviles o de Internet de las cosas (IoT). Además, la evaluación continua de las medidas propuestas en entornos del mundo real sería esencial para validar su efectividad a lo largo del tiempo. En este sentido, ampliar la investigación hacia la interconexión de diferentes modalidades biométricas y su implementación práctica en entornos específicos podría proporcionar una comprensión más completa de la efectividad y la viabilidad de las soluciones propuestas.

5. Conclusiones

Se destaca la gran importancia de abordar las vulnerabilidades en los sistemas biométricos de autenticación en la era digital. Los resultados evidencian que, aunque existen desafíos significativos, también hay soluciones viables y efectivas para mejorar la seguridad y robustez de estos sistemas. La principal vulnerabilidad radica en la constante amenaza de ataques de reproducción y el robo irrevocable de credenciales, especialmente evidente en biometrías oculares.

Se destaca un protocolo biométrico basado en la creación de memoria, que fusiona la biometría ocular y sistemas de desafío, ofreciendo un alto nivel de seguridad y la capacidad de revocar credenciales sin afectar al usuario. Otra estrategia es la implementación de técnicas cancelables en sistemas biométricos, generando plantillas biométricas modificables y temporales para proteger la información biométrica en situaciones cotidianas. Además, la detección de ataques de presentación (PAD) se resalta como una estrategia clave para abordar la vulnerabilidad en diversas modalidades biométricas, asegurando la autenticidad de las interacciones y resistiendo intentos de suplantación. La implementación adecuada de medidas de detección de ataques, tecnologías avanzadas de protección y regulaciones éticas sólidas son pasos cruciales para garantizar una autenticación segura y preservar la privacidad de los usuarios. Además, se enfatiza la necesidad de una inversión continua en investigación y desarrollo para mantenerse al día con las amenazas en constante evolución y fortalecer la seguridad en la autenticación biométrica en un mundo digital en rápido cambio.

La seguridad biométrica avanza mediante la propuesta de soluciones innovadoras y específicas para abordar las vulnerabilidades identificadas. La combinación de enfoques biométricos cancelables, protocolos basados en la creación de memoria y la detección de ataques de presentación ofrece un marco sólido para fortalecer la autenticación biométrica en diversas aplicaciones. Aunque este campo sigue evolucionando, es crucial reconocer que las investigaciones futuras deben enfrentar nuevas amenazas emergentes para garantizar la seguridad continua de las tecnologías biométricas.

6. Referencias Bibliográficas

Ali, S. S., Baghel, V. S., Ganapathi, I. I., & Prakash, S. (2020). Robust biometric authentication system with a secure user template. *Image and Vision Computing*, *104*(104004), 104004. https://doi.org/10.1016/j.imavis.2020.104004

Baig, A. F., Eskeland, S., & Yang, B. (2023). Privacy-preserving continuous authentication using behavioral biometrics. *International Journal of Information Security*, *22*(6), 1833–1847. https://doi.org/10.1007/s10207-023-00721-y

Bera, A., Bhattacharjee, D., & Shum, H. P. H. (2021). Two-stage human verification using HandCAPTCHA and anti-spoofed finger biometrics with feature selection. *Expert Systems with Applications*, *171*(114583), 114583. https://doi.org/10.1016/j.eswa.2021.114583

Bernal-Romero, J. C., Ramirez-Cortes, J. M., Rangel-Magdaleno, J. D. J., Gomez-Gil, P., Peregrina-Barreto, H., & Cruz-Vega, I. (2023). A Review on Protection and Cancelable Techniques in Biometric Systems. *IEEE access: practical innovations, open solutions*, *11*, 8531–8568. https://doi.org/10.1109/access.2023.3239387

Blanchard, N. K., Kachanovich, S., Selker, T., & Waligorski, F. (2020). Reflexive memory authenticator: A proposal for effortless renewable biometrics. En *Lecture Notes in Computer Science* (pp. 104–121). Springer International Publishing. 10.1007/978-3-030-39749-4_7

Bruno, A., Cattaneo, G., Ferraro Petrillo, U., & Capasso, P. (2021). PNU Spoofing: a menace for biometrics authentication systems? *Pattern Recognition Letters*, *151*, 3–10. https://doi.org/10.1016/j.patrec.2021.07.008

De Abiega-L'Eglisse, A. F., Gallegos-Garcia, G., Nakano-Miyatake, M., Rosas Otero, M., & Azpeitia Hernández, V. (2022). A New Fuzzy Vault based Biometric System robust to Brute-Force Attack. *Computación y sistemas*, *26*(3). https://doi.org/10.13053/cys-26-3-4184

Goh, Z. H., Wang, Y., Leng, L., Liang, S.-N., Jin, Z., Lai, Y.-L., & Wang, X. (2022). A framework for multimodal biometric authentication systems with template protection. *IEEE access: practical innovations, open solutions*, *10*, 96388–96402. https://doi.org/10.1109/access.2022.3205413

Goicoechea-Telleria, I., Kiyokawa, K., Liu-Jimenez, J., & Sanchez-Reillo, R. (2019). Low-cost and efficient hardware solution for presentation attack detection in fingerprint biometrics using special lighting microscopes. *IEEE access: practical innovations, open solutions*, *7*, 7184–7193. https://doi.org/10.1109/access.2018.2888905

Gomez-Barrero, M., & Galbally, J. (2020). Reversing the irreversible: A survey on inverse biometrics. *Computers & Security*, *90*(101700), 101700. https://doi.org/10.1016/j.cose.2019.101700

Hernandez-Ortega, J., Fierrez, J., Morales, A., & Galbally, J. (2023). Introduction to presentation attack detection in face biometrics and recent advances. En *Handbook of Biometric Anti-Spoofing* (pp. 203–230). Springer Nature Singapore. https://doi.org/10.1007/978-981-19-5288-3_9

Jain, A. K., Deb, D., & Engelsma, J. J. (2022). Biometrics: Trust, But Verify. *IEEE transactions on biometrics, behavior, and identity science*, *4*(3), 303–323. https://doi.org/10.1109/tbiom.2021.3115465

Joshi, M., Mazumdar, B., & Dey, S. (2020). A comprehensive security analysis of match-in-database fingerprint biometric system. *Pattern Recognition Letters*, *138*, 247–266. https://doi.org/10.1016/j.patrec.2020.07.024

Lee, J., Park, S., Kim, Y.-G., Lee, E.-K., & Jo, J. (2021). Advanced authentication method by geometric data analysis based on user behavior and biometrics for IoT device with touchscreen. *Electronics*, *10*(21), 2583. https://doi.org/10.3390/electronics10212583

Lee, M. J., Teoh, A. B. J., Uhl, A., Liang, S.-N., & Jin, Z. (2021). A tokenless cancellable scheme for multimodal biometric systems. *Computers & Security*, *108*(102350), 102350. https://doi.org/10.1016/j.cose.2021.102350

Mandalapu, H., Reddy P N, A., Ramachandra, R., Rao, K. S., Mitra, P., Prasanna, S. R. M., & Busch, C. (2021). Audio-visual biometric recognition and presentation attack detection: A comprehensive survey. *IEEE access: practical innovations, open solutions*, *9*, 37431–37455. https://doi.org/10.1109/access.2021.3063031

Morales, A., Fierrez, J., Galbally, J., & Gomez-Barrero, M. (2021). *Introduction to Presentation Attack Detection in Iris biometrics and recent advances*. https://doi.org/10.48550/ARXIV.2111.12465

Nakanishi, I., & Maruoka, T. (2019). Biometrics using electroencephalograms stimulated by personal ultrasound and multidimensional nonlinear features. *Electronics*, *9*(1), 24. https://doi.org/10.3390/electronics9010024

Norstrom, P., & Anekanta Consulting. (2021). Has Covid increased public faith in facial recognition? *Biometric Technology Today*, *2021*(11–12), 5–8. https://doi.org/10.1016/s0969-4765(21)00121-1

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. *Journal of Clinical Epidemiology, 134*, 178–189. https://doi.org/10.1016/j.jclinepi.2021.03.001

Sarkar, E., Korshunov, P., Colbois, L., & Marcel, S. (2022). Are GAN-based morphs threatening face recognition? *ICASSP 2022 - 2022 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. https://doi.org/10.1109/ICASSP43922.2022.9746477

Schuiki, J., Linortner, M., Wimmer, G., & Uhl, A. (2022). Attack detection for finger and palm vein biometrics by fusion of multiple recognition algorithms. *IEEE transactions on biometrics, behavior, and identity science*, *4*(4), 544–555. https://doi.org/10.1109/tbiom.2022.3212836

Shukla, D., Kundu, P. P., Malapati, R., Poudel, S., Jin, Z., & Phoha, V. V. (2020). Thinking unveiled: An inference and correlation model to attack EEG biometrics. *Digital Threats: Research and Practice*, *1*(2), 1–29. https://doi.org/10.1145/3374137

Sobabe, A.-A., Djara, T., & Vianou, A. (2020). Biometric system vulnerabilities: A typology of metadata. *Advances in Science Technology and Engineering Systems Journal*, *5*(1), 191–200. https://doi.org/10.25046/aj050125

Tsitiridis, A., Conde, C., Gomez Ayllon, B., & Cabello, E. (2019). Bio-inspired presentation attack detection for face biometrics. *Frontiers in computational neuroscience*, *13*. https://doi.org/10.3389/fncom.2019.00034