Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), septiembre-octubre 2026,
Volumen 10, Número 5.

https://doi.org/10.37811/cl_rcm.v10i5

RECONOCIMIENTO FACIAL CON DETECCIÓN DE VIDA BASADO EN IA PARA CONTROL DE ACCESO EN EDUCACIÓN SUPERIOR

FACIAL RECOGNITION WITH LIVENESS DETECTION BASED ON AI FOR ACCESS CONTROL IN HIGHER EDUCATION

Jesús Abraham Castorena Peña
Universidad Autonoma de Coahuila

Alma Jovita Domínguez Lugo
Universidad Autonoma de Coahuila

Dalia Margarita Alba Cisneros
Universidad Autónoma de Coahuila

Víctor Javier Urbina García
Universidad Autonoma de Coahuila

DOI: https://doi.org/10.37811/cl_rcm.v10i5.26084

Reconocimiento facial con detección de vida basado en IA para control de acceso en educación superior

Jesús Abraham Castorena Peña[1]
jesuscastorenapena@uadec.edu.mx
https://orcid.org/0000-0002-8833-1159
Universidad Autonoma de Coahuila
México

Alma Jovita Domínguez Lugo
almadominguez@uadec.edu.mx
https://orcid.org/0000-0003-4988-4911
Universidad Autonoma de Coahuila
México

Dalia Margarita Alba Cisneros
daliaalba@uadec.edu.mx
https://orcid.org/0009-0009-1033-8244
Centro de Estudios e Investigaciones Interdisciplinarios, Universidad Autónoma de Coahuila, Saltillo, Coahuila, México

Víctor Javier Urbina García
vurbina@uadec.edu.mx
https://orcid.org/0009-0004-1031-1424
Universidad Autonoma de Coahuila
México

RESUMEN

La seguridad en las instituciones de educación superior plantea un desafío; a menudo, el acceso se verifica únicamente mediante credenciales físicas y la supervisión del personal, lo que deja las instalaciones vulnerables a entradas no autorizadas. Esta investigación se centra en el desarrollo y la evaluación de un sistema de reconocimiento facial basado en inteligencia artificial, diseñado principalmente para el control de acceso en instituciones de educación superior. El sistema se desarrolló utilizando el modelo en cascada y una arquitectura de microservicios que comprende una interfaz web en React.js —que emplea MediaPipe FaceMesh para la detección en tiempo real de 478 puntos de referencia faciales—, un servidor en Ruby on Rails para la gestión de datos y un microservicio de IA en Python/FastAPI que incorpora el modelo MiniFASNet para la detección de vitalidad (*liveness detection*) y la biblioteca face_recognition para el reconocimiento facial. Las pruebas contaron con la participación de 50 usuarios y tuvieron en cuenta las condiciones de iluminación y la posible suplantación de identidad; el sistema alcanzó una tasa de éxito del 90%, demostrando un rendimiento superior frente a ataques estáticos en comparación con los intentos de suplantación mediante video. En consecuencia, se confirmó que el sistema funciona eficazmente como herramienta de apoyo para el personal de seguridad y control de acceso.

Palabras clave: Reconocimiento facial; inteligencia artificial; acceso; detección de vida; seguridad

[1] Autor principal
Correspondencia: almadominguez@uadec.edu.mx

Facial recognition with liveness detection based on AI for access control in higher education

ABSTRACT

Security in higher education institutions presents a challenge; often, access is verified solely through physical credentials and staff supervision, leaving the premises vulnerable to unauthorized entry. This research focuses on the development and evaluation of an AI-based facial recognition system designed primarily for access control in higher education institutions. The system was developed using the waterfall model and a microservices architecture comprising a React.js web interface—utilizing MediaPipe FaceMesh for real-time detection of 478 facial landmarks—a Ruby on Rails server for data management, and a Python/FastAPI AI microservice incorporating the MiniFASNet model for liveness detection and the face_recognition library for facial recognition. Testing involved 50 users and accounted for lighting conditions and potential identity spoofing; the system achieved a 90% success rate, demonstrating superior performance against static attacks compared to video-based spoofing attempts. Consequently, the system was confirmed to effectively serve as a support tool for security and access control personnel.

***Keywords*:** Facial recognition; artificial intelligence; access; liveness detection; security

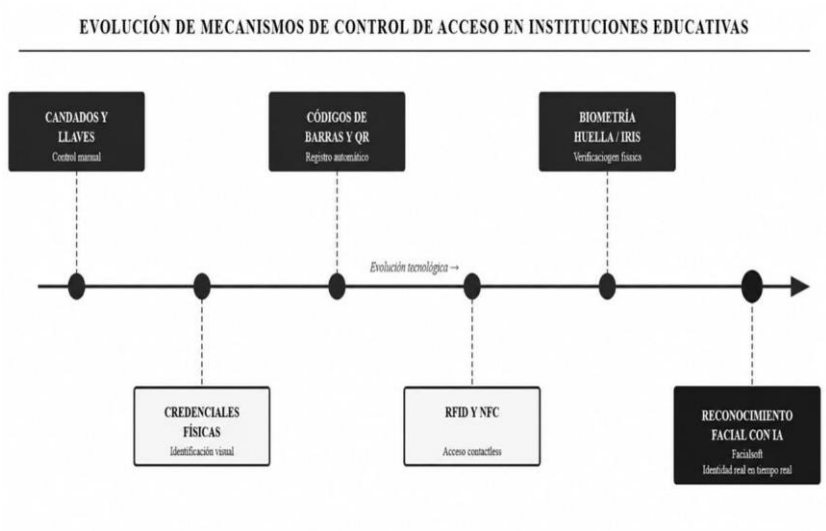
Artículo recibido 06 septiembre 2026
Aceptado para publicación: 07 octubre 2026

INTRODUCCIÓN

Dentro de las instituciones educativas el tema de seguridad es primordial para la comunidad estudiantil, docente y administrativos; algunas asignan la responsabilidad de supervisión a un prefecto para el control de acceso mediante credenciales físicas, listas de asistencia o supervisión directa; estos métodos tradicionales no son suficientes ante la inseguridad que ha venido en aumento en el país.

La dependencia de la supervisión humana en el control de acceso puede generar entornos vulnerables, donde personas ajenas pueden acceder sin ser identificadas correctamente (Anas et al., 2023; Botchway et al., 2024; Mordido, 2025). Botchway et al. (2024), señalan que en años recientes las instituciones han enfrentado niveles crecientes de violencia con respuesta mínima por parte de las autoridades, haciendo necesario y urgente fortalecer los mecanismos de acceso (Figura 1).

Figura 1 *Evolución de los mecanismos de control de acceso en instituciones educativas.*



En el caso de la universidad analizada, el prefecto interviene para cuestionar la presencia de personas ajenas cuando se encuentra en su lugar de trabajo, sin embargo en otros tiempos se encuentra dando rondines principalmente en el área de salones; por lo que, si no está presente, una persona ajena ya ingresó y ha recorrido varios metros dentro de la institución sin ningún tipo de supervisión, cabe mencionar que no es función del prefecto seguir a cada persona que entre. Mordido (2025) documenta que ”El número de personal de seguridad no es suficiente para proteger por completo a todos los visitantes cuando ocurre una amenaza”, además Anas et al. (2023) señalan que “Las cámaras instaladas

solo se utilizan para obtener evidencia, en lugar de prevenir situaciones dentro del campus", reduciendo considerablemente el potencial preventivo de los sistemas de vigilancia. Por esta razón Adiyono et al. (2024) recomiendan invertir en tecnología de vigilancia avanzada, como reconocimiento facial y sistemas que incorporen inteligencia artificial, para una mejor seguridad.

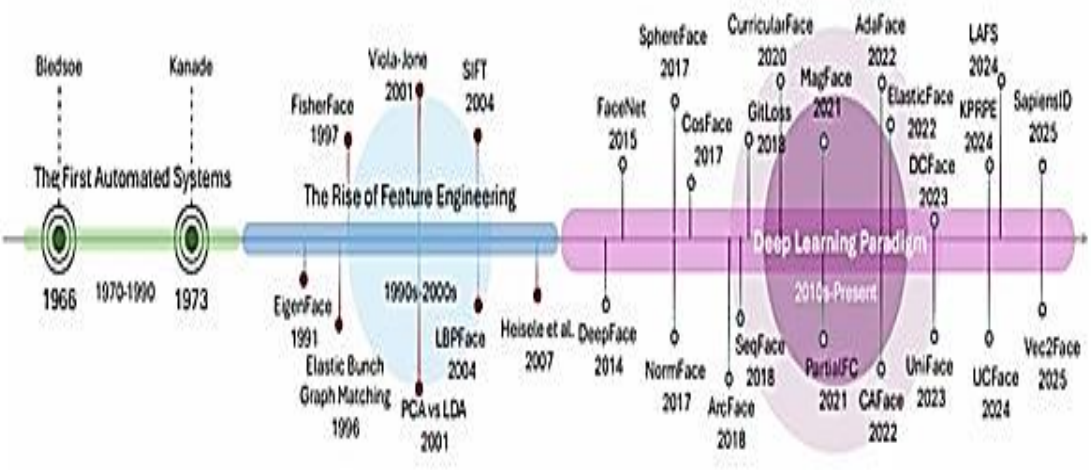
Los mecanismos tradicionales han evolucionado desde sistemas completamente manuales hasta soluciones tecnológicas. Botchway et al. (2024) mencionan que los sistemas de acceso físico han migrado a tecnologías avanzadas de manera inteligente y sistemas biométricos. En donde se automaticen los procesos de acceso para disminuir la dependencia de supervisión humana (Adiyono et al., 2024; Anas et al., 2023; Tinajero et al., 2024). Adiyono et al. (2024) recomiendan "invertir en tecnología de vigilancia avanzada, como reconocimiento facial y sistemas, incorporando inteligencia artificial", para alcanzar a elevar la seguridad.

Con la llegada de la inteligencia artificial y el reconocimiento biométrico, se permite automatizar y fortalecer los procesos de acceso, operando con una cámara estándar de cualquier dispositivo sin altos costos de herramientas especializadas.

La historia del reconocimiento facial ha evolucionado constantemente desde los años 60 Kim et al. (2025) indican que los primeros sistemas surgieron con el trabajo de Woodrow Wilson Bledsoe, quien utilizó landmarks faciales anotados manualmente. A principio de los años noventas el método Eigenfaces basado en análisis de componentes marcó un cambio hacia representaciones holísticas basadas en apariencia.

Figura 2

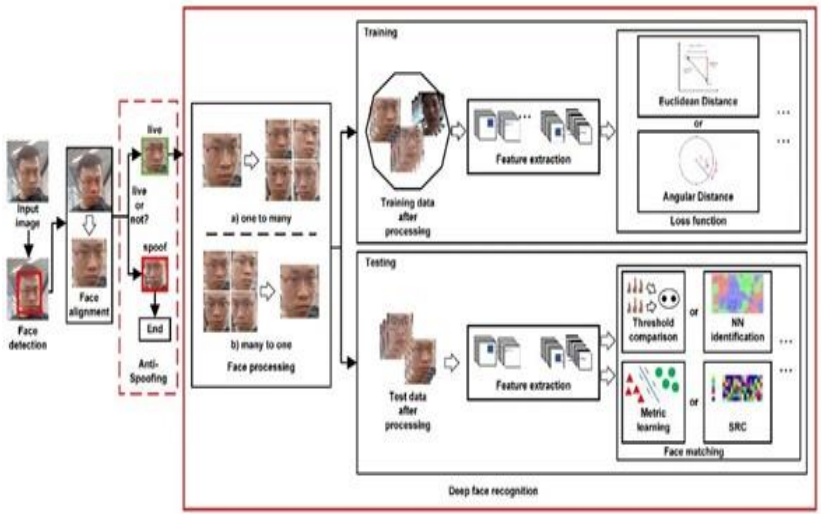
Evolución histórica del reconocimiento facial automatizado a lo largo de cinco décadas.



El reconocimiento facial (Figura 2) es una tecnología biométrica avanzada para la detección y verificación de la identidad de las personas mediante un sistema de análisis automatizado de características faciales. Rukhiran et al. (2023) definen cómo el sistema identifica individuos mediante el análisis de patrones de textura y forma facial. En la Figura 3 se ilustran las etapas generales del proceso de reconocimiento facial.

Figura 3

Etapas generales del proceso de reconocimiento facial.



METODOLOGÍA

El desarrollo se realizó bajo el enfoque de investigación aplicada, con diseño experimental, mediante el uso de una variable independiente (condiciones de iluminación y tipos de ataque de suplantación), para alcanzar a medir el efecto sobre la precisión del sistema. Evaluando además la viabilidad técnica del

sistema para el reconocimiento facial con detección de vida , con el fin de apoyar al personal de control de acceso en la institución educativa.

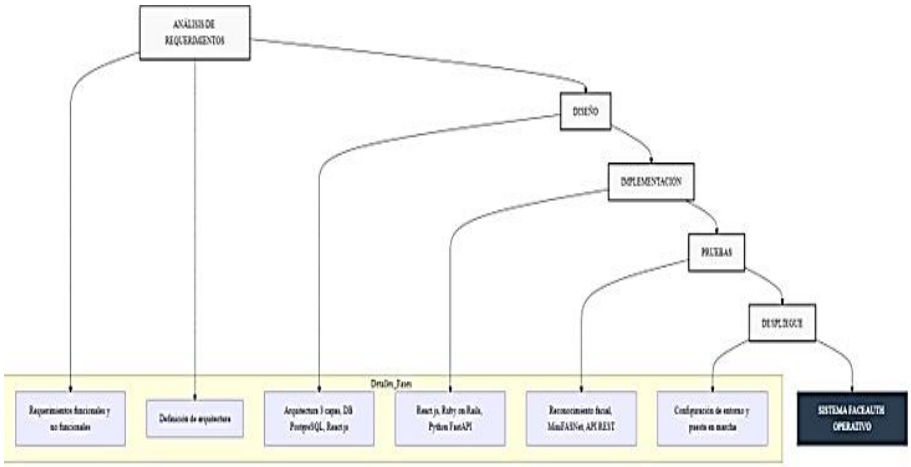
Además, el sistema se rigió mediante la metodología en cascada, tomando en cuenta la propuesta de John & Sharma (2024) por ser adecuado a este tipo de investigaciones con requisitos bien definidos y ciclos de desarrollo secuenciales. Con ello permite estructurar claramente las fases desde el análisis hasta el despliegue (Figura 4)

Para la arquitectura de FaceAuth y siguiendo las recomendaciones de Velepucha & Flores (2023) y Weerasinghe & Perera (2022), quienes señalan la facilidad de escalabilidad , mantenimiento y la posible integración de componentes heterogéneos, se consideró en enfoque de microservicios que consta de tres capas: la implementación en React.js con MediaPipe FaceMesh se encarga de la captura y el análisis de los 478 landmarks del rostro del usuario en tiempo real y se envía del frame al backend de IA; mediante el segundo componente Ruby on Rails se gestionan los registros y administración de los usuarios, y la comunicación entre componentes mediante API REST; y por último mediante Python con FastAPI la inteligencia artificial tiene la responsabilidad de procesar todas las imágenes faciales mediante la librería face_recognition avalando la identificación y MiniFASNet considerando como decisión positiva la clase “life detected” cuando el puntaje de confianza es >=0.85. Para después para la verificación biométrica 1:1 se calcula el embedding de 128 dimensiones utilizando la librería face_recognition a partir del frame capturado y se compara contra el embedding de la plantilla registrada del usuario.

La decisión de coincidencia se realiza con el umbral/tolerance del face_recognition fijado en 0.6 ; por lo tanto se acepta la identidad únicamente si la distancia entre embeddings cumple el criterio definido por dicho umbral..

La arquitectura en capas favoreció la implementación de esta metodología por sus componentes de manera independiente, y trabajar cada fase de forma aislada sin comprometer la integridad de los demás. John y Sharma (2024) definen el modelo como formal de desarrollo de software, también denominado lineal secuencial, donde cada fase debe completarse antes de iniciar la siguiente.

Figura 4 Metodología para el desarrollo de FaceAuth



A través de algoritmos especializados, el sistema es capaz de capturar la imagen y las características faciales de una persona, analizarlas y compararlas con registros almacenados, con el objetivo de reconocer con un alto grado de precisión (Zhao et al., 2003). Tribuana et al. (2024) documentan que ″El modelo entrenado alcanzó una alta precisión de 0.9729 y una baja pérdida de 0.09, demostrando la eficacia del sistema en el control de acceso seguro.", lo que evidencia que los sistemas de reconocimiento facial basados en redes neuronales alcanzan niveles de precisión suficientes para su aplicación en entornos de seguridad institucional. En el proceso de reconocimiento facial en entornos universitarios, el proceso puede mejorar progresivamente la seguridad mediante el acceso automático a las instalaciones, el monitoreo de estudiantes y personal.

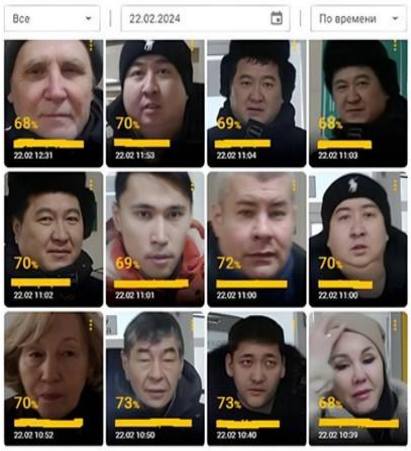
Se involucraron datos biométricos derivados de una muestra de 50 usuarios (N=50), considerando : ser estudiante personal o administrativo , contar con credencial vigente y/o aceptar realizar las pruebas.

Los instrumentos y materiales usados para las mismas, fueron: cámara estándar de dispositivo móvil o webcam integrada, con resolución mínima de 720p, para la captura de la imagen; MediaPipe FaceMesh para la detección de los 478 landmarks faciales en tiempo real; face_recognition para la generación de los encodings faciales de 128 dimensiones; MiniFASNet para la detección de vida , con un umbral de confianza del 0.85; PostgreSQL como gestor de base de datos y React.js, Ruby on Rails y FastAPI como tecnologías de desarrollo.

La detección facial mediante aplicaciones tecnológicas, permiten identificar y localizar el rostro de una persona mediante el análisis de imágenes digitales con algoritmos especializados. Denissova et al. (2025) detallan que los métodos de detección facial incluyen el detector Haar cascade, el detector DNN

en OpenCV y el detector HoG en Dlib, siendo el detector DNN quien demuestra mayor precisión y resistencia al ruido. Por lo que se requieren distintas características para detectar el rostro de una persona, como la forma de cara, grosor de labios , iris, nariz y tamaño del rostro(Figura 5).

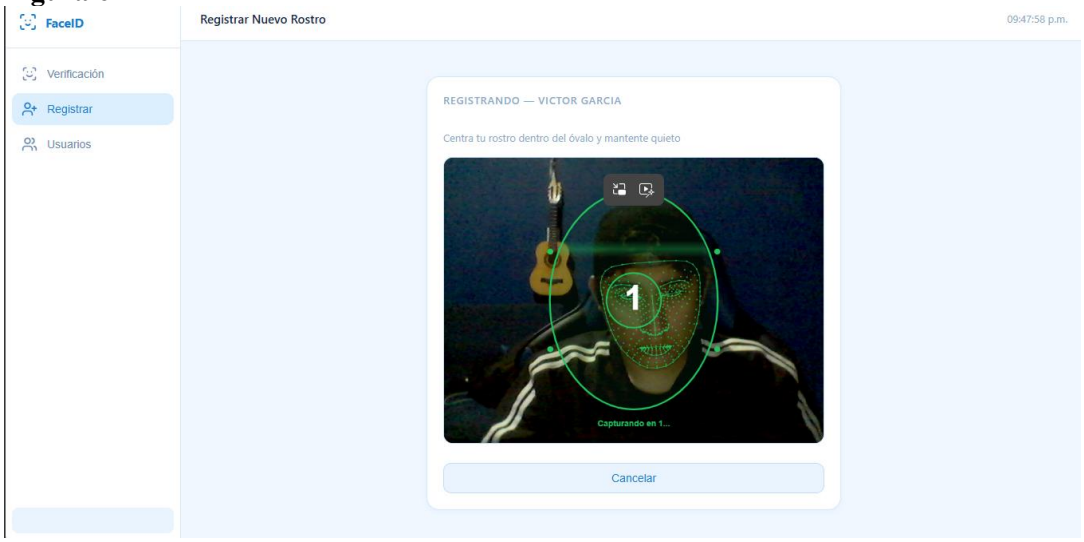
Figura 5 Resultado del módulo de detección facial



RESULTADOS Y DISCUSIÓN

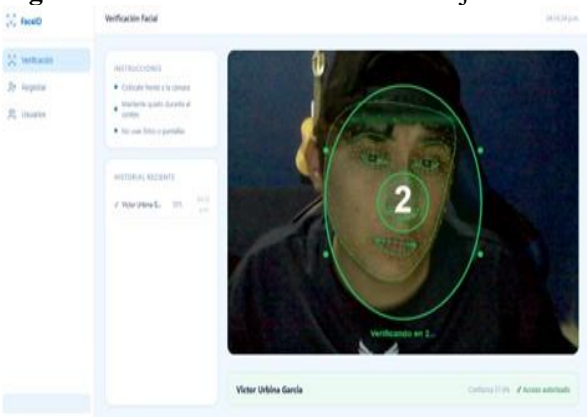
Se registraron los datos generales de usuarios (Figura 6), capturando su rostro bajo condiciones de iluminación controlada, extrayendo los 478 landmarks se generó en encoding facial y se almacenó serializado en PostgreSQL en un tiempo de 4 a 8 segundos.

Figura 6 Interfaz de verificación facial



En la prueba de verificación se realizaron N=50 intentos por condición (50 usuarios * 1 verificación por usuario en cada condición), considerando 10 intentos por usuario en el protocolo agregado y contabilizado por condición el número de coincidencias correctas. Bajo buena iluminación, se obtuvieron 46 coincidencias correctas de luz de 50(92%). Para contraluz, se registraron 33/50 (66%) y para poca luz 7/50 (14%) Tabla 1. Según Kim et al (2023) indica que los modelos de FAS que utilizan únicamente imágenes RGB presentan un bajo rendimiento cuando los conjuntos de datos de entrenamiento y prueba tienen variaciones de luz diferentes, demostrando con ello la limitación inherente de los sistemas basados en cámara RGB.

Figura 7 Verificación facial exitosa bajo condiciones de buena iluminación



Con la identificación de un falso negativo en condiciones de buena iluminación (Figura 7) , se atribuyó a la orientación del rostro en el momento de la captura, pues la leve inclinación de la cabeza reduce considerablemente la precisión del encoding facial mediante la librería face_recognition al momento del registro y compararse con el ángulo de captura durante la verificación. Cuando un usuario es duplicado,

el sistema lo identifica plenamente como el usuario con que comparte una mayor similitud tomando en cuenta las condiciones de captura, pues los encoding fueron generados bajo condiciones muy similares de iluminación y ambiente, lo que resulta en una menor distancia euclidiana entre los vectores de 128 dimensiones. A continuación, se muestran los resultados completos de esta etapa Tabla 1.

Tabla 1. Resultados de pruebas de reconocimiento facial por condición de iluminación

Usuario	**Buena iluminación**	**Contraluz**	**Poca luz**
Usuario 1	9/10	7/10	2/10
Usuario 2	10/10	6/10	1/10
Usuario 3	8/10	7/10	0/10
Usuario 4	9/10	6/10	3/10
Usuario 5	10/10	7/10	1/10
Total	**46/50**	**33/50**	**7/50**
Tasa de éxito	**92%**	**66%**	**14%**

Estos resultados confirman el desempeño que alcanza el sistema, bajo las condiciones óptimas de iluminación, mientras que las variaciones extremas como el contraluz y la poca luz afectan de gran manera la precisión del reconocimiento, así como el comportamiento esperado y documentado. Se calcularon las métricas de rendimiento del sistema las cuales se presentan en la Tabla 3.

En la fase de pruebas de detección de vida, se realizaron 50 pruebas en diferentes escenarios respecto a las fotografías: impresas, de dispositivo estándar, desde pantallas de dispositivo de alta gama, con filtros digitales y videos en reproducción. Este servicio opera mediante el análisis de textura Laplacian combinado con el análisis de saturación HSV como primera capa de verificación, seguido por el modelo MiniFASNet con un umbral de confianza de 0.85 como segunda capa, hasta lograr la aprobación de la imagen cuando se cumplan los requisitos de reconocimiento facial y detección de vida.

En las pruebas con fotografías que usan filtros digitales, se obtuvo una detección del 100%, pues estos alteran las características de textura y saturación de la imagen dificultando el análisis Laplacian aunque sin lograr engañar al sistema. Por último, los videos son un escenario mayormente crítico; en donde se bajó hasta un 70% de detección al permitir el paso de 3 intentos de 10 realizados, con un umbral de

confianza del 0.85. Este resultado confirma que los modelos entrenados se sobreajustan fácilmente a varios dominios y tipos de ataque específicos, y son vulnerables ante dominios no vistos y ataques desconocidos (Ming et al. , 2020), evidenciando que los ataques mediante video de alta calidad representan el vector de ataque más difícil de mitigar con sistemas basados en cámara RGB estándar, según la Tabla 2, en donde se evidencia que el módulo de detección de vida alcanza una tasa de detección global del 90% sobre los 50 intentos de ataques de suplantación.

Tabla 2. Resultados de las pruebas de detección de vida por tipo de ataque

Tipo de ataque	Pruebas	Detectados	Fallos	Tasa de detección
Fotografías impresas	10	10	0	100%
Fotografías pantalla estándar	10	10	0	100%
Fotografías pantalla alta gama	10	8	2	80%
Fotografías con filtros	10	10	0	100%
Videos de reproducción	10	7	3	70%
Total	**50**	**45**	**5**	**90%**

Durante las pruebas de interfaz del usuario, se verificó el correcto funcionamiento, confirmando que los componentes visuales respondieran adecuadamente ante las interacciones del usuario y trabajar de forma clara mostrando los resultados para el personal de vigilancia. Las pruebas de interfaz de usuario mostraron el nombre del usuario, el porcentaje de confianza , el estado de acceso(permitido/denegado) y el historial en tiempo real con fecha y hora.

Para cuantificar el desempeño fue necesario definir las siguientes métricas:

Tasa de verificación exitosa (TVE): Verificaciones correctas / Total de verificaciones × 100.

Tasa de detección de ataques (TDA): Ataques detectados / Total de ataques × 100.

Tabla 3. Métricas derivadas del módulo de liveness

Métrica	Fórmula	Valor
Sensibilidad (TPR)	TP / (TP + FN)	45/50 = 90%

Tasa de falsos negativos (FNR)	FN / (TP + FN)	5/50 = 10%
Precisión de detección	TP / (TP + FP)	45/45 = 100%
Especificidad (TNR)	TN / (TN + FP)	No calculable

CONCLUSIONES

Después del desarrollo del sistema de reconocimiento facial, con la integración de los tres elementos React.js, Ruby on Rails y Python con FastAPI, se demuestra que el trabajo en conjunto permitió al sistema alcanzar una tasa de reconocimiento del 92% bajo condiciones de buena iluminación, y las diferencias entre los casos presentados se atribuyen principalmente a las condiciones de hardware disponible durante las pruebas, pues depende ampliamente de las condiciones de cámara y su capacidad de procesamiento. Además es importante señalar que FaceAuth contempla simultáneamente detección de vida y reconocimiento facial en una arquitectura de tres capas que opera en tiempo real, representando esto una contribución diferencial del sistema ante los existentes.

Con ello se demuestra que la arquitectura de microservicios es la más adecuada para este tipo de sistemas biométricos Velepucha & Flores (2023) y Weerasinghe & Perera (2022). La integración de MediaPipe FaceMesh para la detección de 478 landmarks faciales representa una decisión acertada de diseño, reduciendo la carga computacional del servidor y sobre todo alcanzar los tiempos de respuesta óptimos incluso en dispositivos con recursos limitados.

Lo anterior fue mediante la implementación de modelos de inteligencia artificial al lograr identificar si una fotografía pertenece a una persona físicamente presente y no a un intento de suplantación de identidad con fotografías impresas o en pantallas de dispositivos.

Así mismo, la detección de vida alcanzó una tasa global del 90% en los escenarios evaluados.

En general, el sistema demuestra ser una solución funcional y viable para apoyo a elementos de vigilancia para el control de acceso en instituciones educativas.

REFERENCIAS BIBLIOGRÁFICAS

Adiyono, A., Mandasari, K., Laila, N. A., & Suryani, N. Y. (2024). *School facility security: An evaluation of surveillance technologies and efforts to improve physical security*. *International Education Trend Issues, 2*(1), 65–75. https://ijble.com/index.php/ieti

Anas, A., Aliyu, M., Ismail, A. B., Bakale, M. A., Yeldu, Z. Y., Sidi, A., Ahmad, A., & Aliyu, A. (2023). *Safe campus: An intelligent campus video surveillance system for crowd analysis*. *Dutse Journal of Pure and Applied Sciences, 9*(1b), 103–109. https://doi.org/10.4314/dujopas.v9i1b.10

Botchway, E. A., Agyekum, K., Pittri, H., & Lamina, A. (2024). *Deployment of physical access control (PAC) devices in university settings in Ghana*. *Frontiers in Engineering and Built Environment, 4*(1), 1–14. https://doi.org/10.1108/FEBE-01-2023-0006

Denissova, N., Dyomina, I., Tlebaldinova, A., & Apayev, K. (2025). *Enhancement of the facial recognition module in the "Safe University" system through adaptive fine-tuning*. *Journal of Advances in Information Technology, 16*(1), 144–155. https://doi.org/10.12720/jait.16.1.144-155

John, J. J., & Sharma, S. S. (2024). *A comparative study of agile and waterfall software development methodologies*. *International Journal of Advanced Research in Science, Communication and Technology, 4*(2), 54–57. https://doi.org/10.48175/IJARSCT-15207

Kim, M., Jain, A., & Liu, X. (2025). *50 years of automated face recognition*. *arXiv*. https://arxiv.org/abs/2505.24247

Kim, Y., Gwak, H., Oh, J., Kang, M., Kim, J., Kwon, H., & Kim, S. (2023). *CloudNet: A LiDAR-based face anti-spoofing model that is robust against light variation*. *IEEE Access, 11*, 16984–16992. https://doi.org/10.1109/ACCESS.2023.3242654

Ming, Z., Visani, M., Luqman, M. M., & Burie, J. C. (2020). *A survey on anti-spoofing methods for facial recognition with RGB cameras of generic consumer devices*. *Journal of Imaging, 6*(12), 139. https://doi.org/10.3390/jimaging6120139

Mordido, J. C. (2025). *Analyzing institutional security measures: Implementation, effectiveness, and challenges*. *EPRA International Journal of Multidisciplinary Research, 11*(12), 216–220. https://doi.org/10.36713/epra25270

Rukhiran, M., Wong-In, S., & Netinant, P. (2023). *IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach*. *IEEE Access, 11*, 22767–22787. https://doi.org/10.1109/ACCESS.2023.3253024

Tinajero Juárez, B. Y., Barrera Argumedo, E., González Islas, J. C., Freyri Maya Gress, K., & Espinoza Santander, J. R. (2024). *Control de acceso local sistema seguro para estudiantes*. *Innovación y Ciencia, 4*(4). https://doi.org/10.63371/ic.v4.n4.a595

Tribuana, D., Hazriani, & Arda, A. L. (2024). *Face recognition for smart door security access with convolutional neural network method*. *TELKOMNIKA Telecommunication Computing Electronics and Control, 22*(3), 702–710. https://doi.org/10.12928/TELKOMNIKA.v22i3.25946

Velepucha, V., & Flores, P. (2023). *A survey on microservices architecture*. *IEEE Access, 11*, 88339–88358. https://doi.org/10.1109/ACCESS.2023.3305687

Weerasinghe, L. D. S. B., & Perera, I. (2022). *Evaluating the inter-service communication on microservice architecture*. En *Proceedings of the 2022 7th International Conference on Information Technology Research (ICITR)* (pp. 1–6). IEEE. https://doi.org/10.1109/ICITR57877.2022.9992918

Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). *Face recognition: A literature survey*. *ACM Computing Surveys, 35*(4), 399–458. https://doi.org/10.1145/954339.954342