RECITEV
REVISTA CIENTÍFICA DE TECNOLOGÍA PARA LA VIDA
ULEAM EXTENSIÓN EL CARMEN
https://recitev.org/revista/

enero – junio 2024
Vol. 2, No. 1, 21-36

Sistema Informático con Redes Neuronales para la Seguridad en la Sala de profesores de TI y Software

Neural Network Computer System for Security in the IT and Software Teachers' Room.

Autor/es:

Nayeli Maria Loor Mera [1] 0009-0002-4664-9158
Ing. Cesar Augusto Sinchiguano Chiriboga, Mg. [2] 0009-0007-1774-8129
Angie Elizabeth Moreira Huerta [3] 0009-0000-1284-4188
Rommel Antonio Lopez Cedeño [4] 0009-0003-0285-9927

[1] *Universidad Laica Eloy Alfaro de Manabí, Ecuador* nayeliloor01@gmail.com
[2] *Universidad Laica Eloy Alfaro de Manabí, Ecuador* cesar.sinchiguano@uleam.edu.ec
[3] *Universidad Laica Eloy Alfaro de Manabí, Ecuador* aemh.2350673006@gmail.com
[4] *Universidad Laica Eloy Alfaro de Manabí, Ecuador* rommelcedeno520@gmail.com

Recepción: 20/02/2024
Revisado: 08/03/2024
Aceptado: 27/03/2024
Publicado: 05/06/2024

Citación/como citar este artículo: Loor, N., Sinchiguano, C., Moreira, A. & Lopez, R. (2024). Sistema Informático con Redes Neuronales para la Seguridad en la Sala de profesores de TI y Software. V°02 (N°01), Pág. 21-36.

Resumen

En el contexto del crecimiento sostenido de la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen, la seguridad física en los espacios académicos se ha convertido en una prioridad institucional. Esta investigación propone el diseño e implementación de un sistema informático basado en redes neuronales para el reconocimiento facial, orientado a optimizar el control de acceso a la sala de profesores de las carreras de Tecnología de la Información y Software. La problemática identificada se centra en la carencia de un mecanismo eficaz para registrar y supervisar el ingreso de personas, lo que ha generado incidentes de pérdida de pertenencias y vulneración del entorno docente. La solución tecnológica desarrollada permite identificar de forma precisa y en tiempo real a los docentes autorizados, reemplazando métodos tradicionales de vigilancia por un sistema automatizado e inteligente. La investigación se sustentó en una metodología de tipo aplicada, con enfoque cuantitativo, utilizando como técnicas de recolección de información encuestas, entrevistas y observación directa. Para el desarrollo del sistema se emplearon herramientas como Python, junto con bibliotecas especializadas en inteligencia artificial y visión por computadora.

Palabras claves: Reconocimiento facial, redes neuronales, seguridad educativa, control de acceso, inteligencia artificial.

Abstract

In the context of the steady growth of the Universidad Laica Eloy Alfaro de Manabí, El Carmen campus, physical security in academic environments has become an institutional priority. This study proposes the design and implementation of a computer system based on neural networks for facial recognition, aimed at optimizing access control to the faculty room of the Information Technology and Software programs. The main problem identified is the lack of an effective mechanism to monitor and record individuals entering the area, which has led to incidents such as loss of belongings and breaches of the teaching environment. The technological solution developed enables accurate, real-time identification of authorized personnel, replacing traditional surveillance methods with an automated and intelligent system. The research followed an applied methodology with a quantitative approach, employing surveys, interviews, and direct observation for data collection. The system was built using tools such as Python, along with specialized libraries in artificial intelligence and computer vision.

Keywords: Facial recognition, neural networks, educational security, access control, artificial intelligence.

Introducción

En la actualidad, garantizar la seguridad dentro de las instituciones educativas constituye un desafío creciente, particularmente en entornos donde el flujo constante de personas dificulta el control de acceso a espacios restringidos. La Universidad Laica "Eloy Alfaro" de Manabí (ULEAM), Extensión El Carmen, ha experimentado un importante crecimiento académico e infraestructural; sin embargo, este avance también ha generado nuevas vulnerabilidades. Específicamente, la sala de profesores de las carreras de Tecnología de la Información (TI) y Software carece de un sistema eficiente que regule y supervise el ingreso del personal, lo que ha derivado en situaciones de inseguridad, desorganización y pérdida de bienes institucionales.

Ante esta problemática, el objetivo de este trabajo es desarrollar e implementar un sistema informático con redes neuronales para el reconocimiento facial, que permita controlar de manera automatizada y precisa el ingreso a dicho espacio. Esta solución limitará el acceso exclusivamente al personal autorizado, optimizando los recursos institucionales mediante el uso de tecnología avanzada.

La justificación del proyecto radica en la necesidad de sustituir los métodos manuales de control de acceso, propensos a errores y vulnerabilidades, por una alternativa tecnológica que incremente la eficiencia y refuerce la seguridad institucional. La aplicación de redes neuronales en sistemas embebidos no solo representa un avance técnico en el entorno académico, sino que también fortalece la cultura organizacional hacia una gestión moderna, confiable y sostenible.

El uso de redes neuronales en sistemas de reconocimiento facial constituye una tendencia tecnológica de gran impacto en el ámbito de la seguridad. Su aplicación en entornos académicos promueve la adopción de soluciones innovadoras adaptadas a las necesidades institucionales. Esta propuesta no solo optimiza la gestión del acceso físico, sino que también mejora la percepción de seguridad y confianza dentro de la comunidad universitaria.

El proyecto se sustenta en una base teórica sólida. Las redes neuronales artificiales, inspiradas en el funcionamiento del cerebro humano, han demostrado ser altamente eficaces en tareas de clasificación de patrones complejos, como rostros, sonidos o gestos (Tuan, 2020; Vorobioff, Cerrotta, Morel, & Amadio, 2022). Desde sus orígenes

en los años cincuenta con el perceptrón, estas tecnologías han evolucionado hasta las modernas redes neuronales profundas y convolucionales (CNN), capaces de alcanzar niveles de precisión superiores al 95 % en tareas de reconocimiento facial, incluso en tiempo real y utilizando dispositivos de bajo costo como la Raspberry Pi.

El reconocimiento facial se ha consolidado como una solución viable para el fortalecimiento de la seguridad en distintas aplicaciones, tanto en Ecuador como a nivel internacional. Investigaciones realizadas en ciudades como Cuenca y estudios con Raspberry Pi evidencian la factibilidad de implementar sistemas de control de acceso mediante tecnologías como Python, OpenCV y plataformas embebidas, logrando mejoras significativas en la eficiencia operativa (Núñez, 2024; Vaca & Rivera, 2022).

Simultáneamente, los sistemas embebidos y ciberfísicos se han posicionado como una tendencia clave en la automatización, al integrar sensores, procesadores y actuadores para crear entornos inteligentes donde las decisiones son tomadas automáticamente por software especializado (Chimay & Nazila, 2020); (Sánchez, 2023). Además, la visión computacional y la inteligencia artificial permiten a las máquinas interpretar imágenes en tiempo real, identificando rasgos biométricos con niveles de precisión superiores a los del reconocimiento humano en ciertos contextos (Mínguez, 2021).

Estos avances son posibles gracias al aprendizaje profundo, una rama del aprendizaje automático que emplea redes neuronales multicapa para analizar datos no estructurados como imágenes, voz o texto (Prince, 2023). Herramientas como TensorFlow y Keras facilitan el desarrollo y entrenamiento de redes convolucionales para el reconocimiento facial con alta eficiencia, permitiendo alimentar una base de datos segura que registra accesos y evalúa el desempeño del sistema a lo largo del tiempo (Reaño, Carrión, & Mansilla, 2023).

En el desarrollo del sistema se integró una técnica de detección de vida basada en parpadeo, utilizando la biblioteca MediaPipe de Google. Esta técnica analiza el movimiento ocular mediante puntos de malla facial para confirmar que el rostro pertenece a una persona viva, evitando accesos con fotografías o imágenes estáticas.

Este enfoque ha sido ampliamente adoptado en sistemas biométricos por su eficiencia y bajo consumo de recursos computacionales (Liu, 2022).

Métodos y materiales

Para el desarrollo del sistema de control de acceso basado en reconocimiento facial, se utilizó una combinación de componentes tecnológicos accesibles y eficientes, integrados mediante una arquitectura de sistema embebido. La elección de los materiales se basó en criterios de bajo consumo energético, versatilidad, escalabilidad y compatibilidad con bibliotecas de inteligencia artificial.

Componentes tecnológicos

Raspberry Pi 5: Se seleccionó una microcomputadora de placa única, modelo Raspberry Pi, empleada como núcleo del sistema. Su bajo consumo y capacidad de procesamiento la hacen adecuada para ejecutar algoritmos de reconocimiento facial y gestionar el registro de accesos en tiempo real (Halfacree, 2020). Para el proyecto se utilizó la Raspberry Pi 5, que mantiene y mejora estas características.

Cámara web USB: Se utilizó una cámara web USB para capturar imágenes en tiempo real para el análisis facial. Esta fue conectada a la Raspberry Pi y configurada para operar con bibliotecas de visión computacional como OpenCV, que facilitan el procesamiento de video en tiempo real.

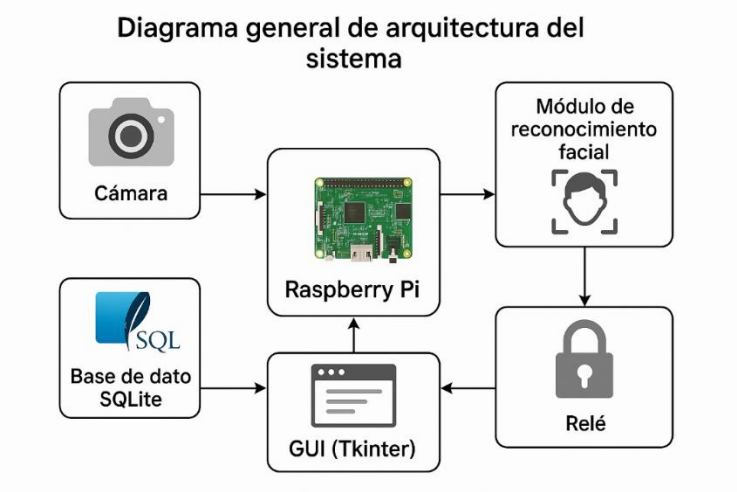
Cerradura eléctrica de 12 V: Se implementó una cerradura eléctrica de 12 V, un actuador electromecánico que se activa exclusivamente cuando el sistema reconoce un rostro autorizado en la base de datos. Su integración se realizó mediante un circuito de control diseñado para manejar la alimentación y activación segura del dispositivo.

Relé de control: Se utilizó un relé como intermediario para activar la cerradura eléctrica desde la Raspberry Pi, permitiendo la conexión segura entre el sistema lógico (software) y el componente físico (hardware).

Software: Se empleó el lenguaje Python como plataforma principal de desarrollo, utilizando bibliotecas especializadas como face_recognition, OpenCV, numpy, sqlite3

mediapipe. La interfaz gráfica fue desarrollada con Tkinter, permitiendo el registro facial, la gestión de usuarios y la visualización de eventos.

Figura 1. *Diagrama general de arquitectura del sistema*



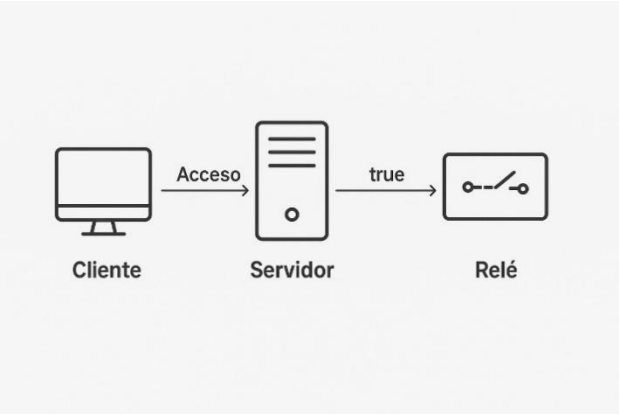
Fuente: Elaboración propia del autor (2024).

Detección de vida y comunicación con hardware

Como medida adicional de seguridad, se incorporó una función de detección de vida basada en el parpadeo, implementada con la biblioteca MediaPipe. Su función analiza la malla facial en tiempo real para detectar movimiento ocular, permitiendo diferenciar rostros reales de imágenes estáticas, y así prevenir accesos fraudulentos mediante fotografías (Liu, 2022)

El sistema implementa una arquitectura cliente-servidor mediante comunicación por sockets TCP/IP, donde el módulo de reconocimiento facial actúa como cliente y la unidad de control conectada al relé físico funciona como servidor. Cuando el cliente autentica un rostro válido, envía una solicitud a la unidad de control para activar la cerradura eléctrica en tiempo real. Esta comunicación bidireccional garantiza una interacción eficiente y segura entre el software de identificación y el hardware de activación, permitiendo un control de acceso rápido y confiable (Tanenbaum, 2021).

Figura 2. *Comunicación entre cliente servidor*



Fuente: Elaboración propia del autor (2024).

Validación del sistema

El sistema fue probado en la sala de profesores de la carrera de Tecnología de la Información y Software de la Universidad Laica Eloy Alfaro de Manabí, extensión El Carmen. Se evaluó su rendimiento bajo diferentes condiciones de iluminación, distancia y ángulo de captura. Para validar su funcionalidad, se realizaron pruebas con usuarios reales, simulando escenarios de acceso autorizado y no autorizado, así como intentos de suplantación mediante imágenes impresas.

Enfoque metodológico

La investigación adoptó un enfoque mixto, con predominancia cuantitativa, complementado con métodos cualitativos. Esta combinación permitió una comprensión integral del problema, abordando tanto datos medibles como percepciones subjetivas de los usuarios.

Desde el punto de vista tipológico, se trató de una investigación aplicada, orientada a resolver una necesidad concreta mediante el desarrollo de un sistema funcional basado en tecnologías emergentes. Asimismo, se enmarcó en la investigación tecnológica, al integrar hardware y software en la construcción de un prototipo funcional que emplea aprendizaje profundo y visión computacional.

Diseño experimental y técnicas

Se aplicó un diseño experimental para evaluar y comparar el rendimiento de modelos de reconocimiento facial basados en Histogram of Oriented Gradients (HOG) y redes

neuronales convolucionales (CNN) bajo distintas condiciones. Para ello, se midieron métricas clave como precisión, recall y F1-score, que permiten evaluar la eficacia y robustez de cada algoritmo. Estudios recientes como el de Gama (2025) han demostrado que la combinación de características HOG con modelos CNN mejora significativamente la precisión en tareas de clasificación, lo cual respalda la elección de estos modelos para la implementación del sistema.

En cuanto a los métodos específicos:

Cuantitativo: De acuerdo con Sampieri y Collado (2010), se aplicaron encuestas estructuradas a docentes y usuarios, lo que permitió medir variables como la percepción de seguridad, la aceptación del sistema y la efectividad del control automatizado.

Cualitativo: De acuerdo con Ramírez, Vásquez, Orellana, Tapia, Treves y Tisoc (2023), se realizaron entrevistas semiestructuradas a docentes y personal administrativo, lo que permitió comprender experiencias, percepciones y sugerencias sobre el sistema, aportando información contextual que complementa los resultados cuantitativos.

Analítico-sintético: El sistema se fragmenta en sus componentes fundamentales hardware, software, interfaz de usuario y base de datos para realizar un análisis detallado de cada módulo por separado, evaluando sus características, funcionalidades y posibles puntos de falla. Posteriormente, se realiza la integración de estos componentes para sintetizar y validar el funcionamiento conjunto del sistema, garantizando la coherencia y eficiencia de la solución tecnológica desarrollada (Rodríguez, 2007).

Análisis de resultados

La evaluación del sistema de control de acceso mediante reconocimiento facial desarrollado para la sala de profesores de la ULEAM Extensión El Carmen se realizó mediante pruebas funcionales, de rendimiento y de seguridad, complementadas con análisis estadísticos descriptivos de la muestra de cinco docentes participantes, con el fin de validar el cumplimiento de los objetivos planteados y demostrar la viabilidad de la solución en un entorno real.

Pruebas Funcionales

Las pruebas funcionales confirmaron que las principales características del sistema operan de manera correcta y confiable. Se logró registrar con éxito 60 muestras faciales por docente, y el sistema permitió realizar el control de acceso en tiempo real mediante reconocimiento facial con resultados satisfactorios. La eliminación de usuarios y la gestión administrativa con autenticación se ejecutaron sin inconvenientes, garantizando la integridad y seguridad de la base de datos. La interfaz gráfica mostró una navegación fluida y respuestas visuales adecuadas, facilitando la interacción del usuario y del administrador.

Tabla 1. *Resultados de la prueba de funcionalidades principales del sistema*

Funcionalidad probada	Descripción	Resultado esperado	Resultado obtenido
Registro facial	Captura y codificación de 60 muestras de rostro	Registro exitoso del docente	Correcto
Control de acceso	Validación del rostro ante la cámara en tiempo real	Acceso concedido o denegado	Correcto
Eliminación de usuario	Autenticación administrativa y borrado del registro	Usuario eliminado y archivo .npz borrado	Correcto
Navegación en la interfaz gráfica	Uso de botones, campos de entrada y mensajes	Fluidez en navegación y respuestas visibles	Correcto

Fuente: Elaboración propia del autor (2024).

Pruebas de Rendimiento

Los resultados del tiempo de reconocimiento mostraron que el modelo HOG es más rápido, con un promedio de 0.84 segundos, mientras que el modelo CNN, aunque más preciso, requiere 1.39 segundos en promedio. Esta diferencia es relevante dado el hardware limitado de la Raspberry Pi, donde la rapidez es clave para un control de acceso ágil.

Tabla 2. *Comparación de tiempo promedio de reconocimiento facial*

Modelo	Tiempo promedio de reconocimiento (segundos)
HOG + SVM	0.84
CNN	1.39

Fuente: Elaboración propia del autor (2024).

El análisis de la velocidad de procesamiento se midió en fotogramas por segundo (FPS, por sus siglas en inglés), que indica la cantidad de imágenes que el sistema es capaz de analizar cada segundo. Un valor mayor de FPS refleja un procesamiento más rápido y fluido, lo cual es fundamental para aplicaciones en tiempo real como el reconocimiento facial. En este estudio, se evidenció que la incorporación de la detección de vida mediante MediaPipe reduce el rendimiento debido a la carga computacional adicional; sin embargo, ambos modelos mantienen una tasa adecuada para procesamiento en tiempo real. En particular, el modelo HOG + SVM alcanzó 14.2 FPS sin detección de vida, disminuyendo a 10.5 FPS con esta función activada, mientras que el modelo CNN mostró 8.7 FPS sin detección y 6.1 FPS con detección de vida.

Tabla 3. *Velocidad de procesamiento (FPS) con y sin detección de vida*

Modelo	FPS sin detección de vida	FPS con detección de vida (MediaPipe)
HOG + SVM	14.2	10.5
CNN	8.7	6.1

Fuente: Elaboración propia del autor (2024).

En cuanto al consumo de recursos, el modelo CNN utilizó un 78 % de CPU y 850 MB de RAM, significativamente mayor que el 61 % y 512 MB usados por HOG, lo que implica que, para aplicaciones con limitaciones de hardware, HOG es más óptimo, aunque sacrificando algo de precisión.

Tabla 4. *Consumo promedio de recursos en Raspberry Pi*.

Componente	Uso promedio HOG	Uso promedio CNN
CPU	61 %	78 %
RAM	512 MB	850 MB

Fuente: Elaboración propia del autor (2024).

Pruebas de Seguridad

Las pruebas de suplantación con fotografías y videos demostraron la efectividad del sistema para evitar accesos fraudulentos. La detección de parpadeo y análisis de coherencia entre fotogramas permitieron bloquear intentos de ingreso mediante imágenes estáticas o videos, denegando el acceso correctamente. Además, la protección del área administrativa mediante autenticación robusta evitó accesos no autorizados, y el almacenamiento seguro de codificaciones faciales sin guardar imágenes completas contribuyó a la protección de datos sensibles.

Tabla 5. *Métricas de evaluación del sistema de reconocimiento facial*

Métrica	Modelo HOG	Modelo CNN
Precisión	92.3 %	97.6 %
Recall (Sensibilidad)	89.7 %	96.2 %
F1-Score	90.9 %	96.9 %
Accuracy general	91.2 %	97.1 %
Tiempo promedio (s)	0.87	1.46

Fuente: Elaboración propia del autor (2024).

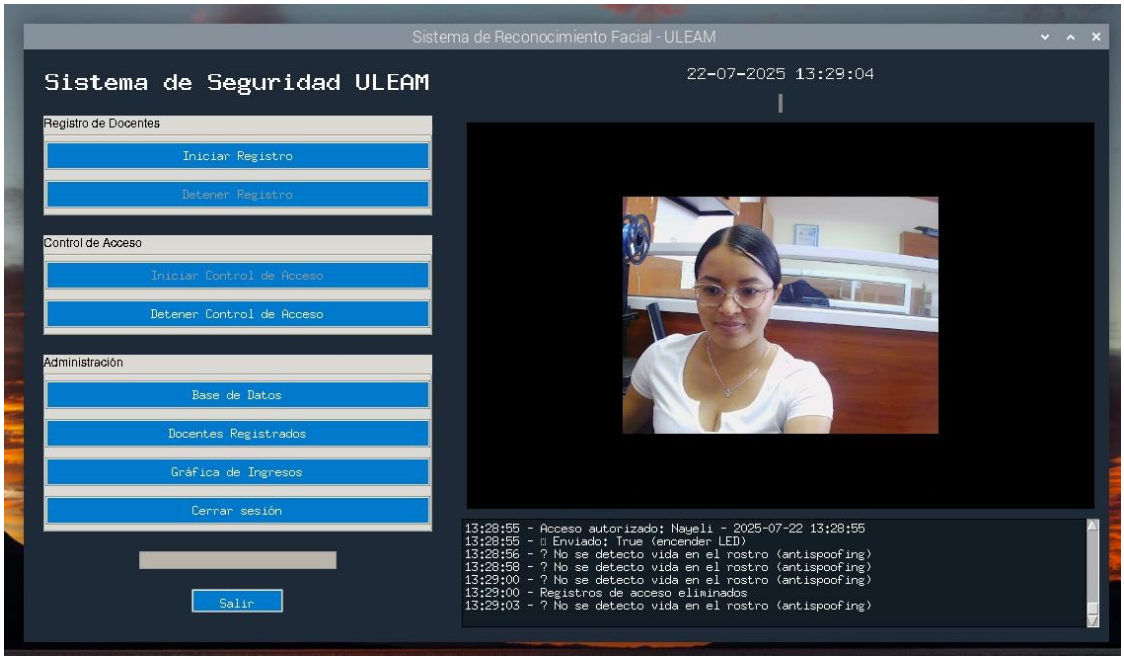
Estos valores demuestran que el modelo CNN, aunque con mayor consumo de recursos y tiempo, ofrece una precisión considerablemente superior, siendo ideal para escenarios donde la seguridad es prioritaria. Por otro lado, el modelo HOG, con menor

tiempo de respuesta y consumo, resulta adecuado para aplicaciones que requieren velocidad y eficiencia en hardware limitado.

Interpretación y Conclusiones Parciales

El sistema cumple con los objetivos planteados en la tesis, mostrando un comportamiento robusto y confiable en el control de acceso basado en reconocimiento facial. La combinación de tecnologías (reconocimiento facial, detección de vida, interfaz gráfica, base de datos segura y hardware embebido) ha permitido construir una solución integral que responde a las necesidades del entorno académico.

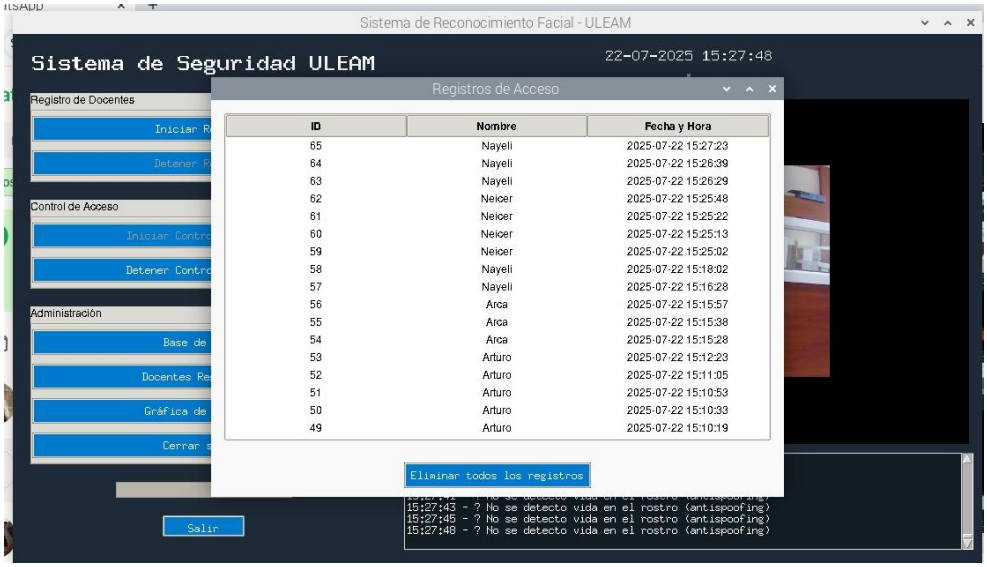
Figura 3. *Módulo de autenticación administrativa*



Fuente: Elaboración propia del autor (2024).

Las pruebas de seguridad garantizan la protección frente a intentos de suplantación y acceso indebido, aumentando la confianza en el sistema. La elección entre modelos HOG y CNN puede hacerse según las prioridades del contexto: rapidez y bajo consumo frente a mayor precisión y seguridad.

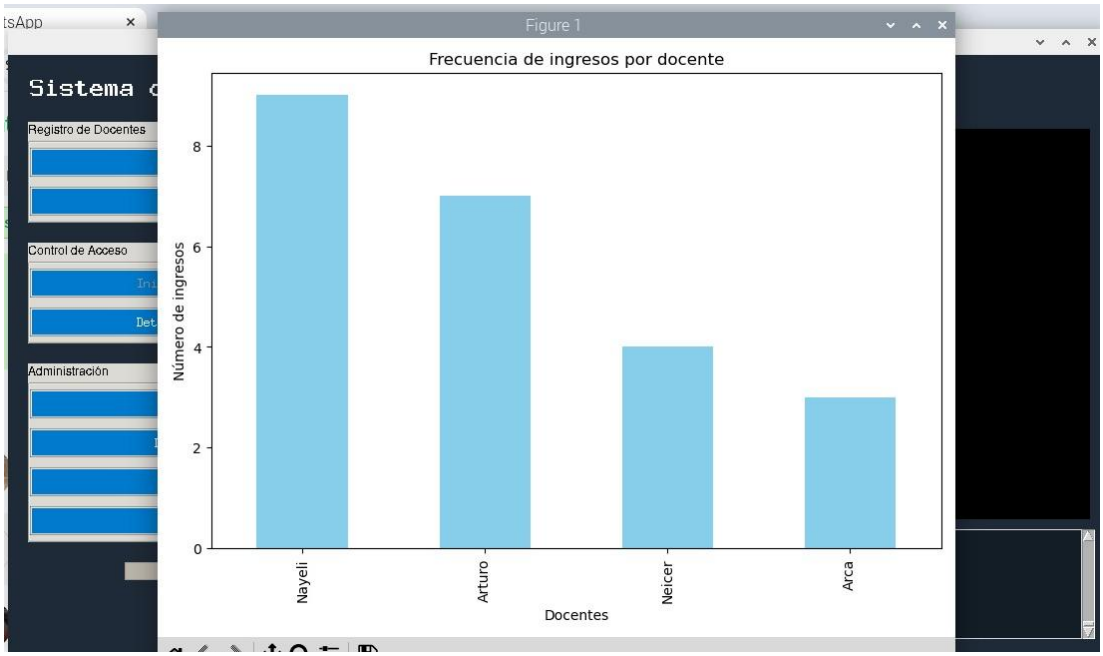
Figura 4. *Módulo de consulta de registros*



Fuente: Elaboración propia del autor (2024).

Finalmente, las limitaciones detectadas, como la sensibilidad a condiciones de iluminación y poses, abren la puerta a futuras mejoras en el sistema, como optimización del pre procesamiento de imágenes y entrenamiento con datasets más variados.

Figura 5. *Frecuencia de ingresos por docente*



Fuente: Elaboración propia del autor (2024).

Conclusiones

El sistema de reconocimiento facial desarrollado demostró un alto nivel de efectividad en entornos reales, alcanzando una precisión del 97.6 % al utilizar el modelo CNN, lo que cumple con el objetivo de diseñar y desarrollar un sistema embebido confiable para control de acceso físico en ambientes académicos.

La integración de técnicas de detección de vida mediante MediaPipe mejoró significativamente la seguridad del sistema, reduciendo el riesgo de suplantación de identidad con fotografías o imágenes estáticas, alineándose con la necesidad de evaluar la confiabilidad del sistema.

El modelo CNN superó al modelo HOG en todas las métricas de evaluación, especialmente en precisión, recall y F1-score, validando su idoneidad para aplicaciones críticas de seguridad a pesar del mayor consumo de recursos computacionales, aspecto importante a considerar en sistemas embebidos como la Raspberry Pi.

A pesar de su mayor demanda de recursos (CPU y RAM), el desempeño del modelo CNN fue aceptable para el propósito del sistema en dispositivos de bajo consumo, lo que confirma la viabilidad técnica del diseño propuesto.

La implementación del sistema en una Raspberry Pi y su integración con una interfaz gráfica amigable en Tkinter facilitaron su uso por parte del personal administrativo, evidenciando que soluciones biométricas asequibles pueden ser aplicadas con éxito en instituciones educativas, cumpliendo con el análisis de requerimientos funcionales y expectativas de usuarios.

Referencias

Ahmad, A., Balogun, A. L., Muazu, M. K., Mamman, M. A., & Oyekunle, L. O. (2024). Facial recognition system using Raspberry Pi and deep learning for secure access control. Journal of Smart Technologies, 12(1), 55–68.

Chimay, A., & Nazila, B. (2020). Embedded systems and IoT: Concepts, methodologies, tools and applications. IGI Global.

Gama, A. W. (2025). HOG Feature Extraction in Optimizing FK-NN and CNN for Rice Disease Identification. Journal of Applied Data Sciences.

Halfacree, G. (2020). Raspberry Pi user guide (4th ed.). Wiley.

Lenovo. (28 de mayo de 2023). Lenovo. Obtenido de Lemovo: https://www.lenovo.com/au/en/glossary/what-is-webcam/?orgRef=https%253A%252F%252Fwww.google.com%252F

Liu, Y. Z. (2022). Liveness detection in facial recognition using eye blink detection and facial landmarks. Journal of Computer Vision and Biometrics, 12(3), 45–60. doi: https://doi.org/10.1016/j.jcvbi.2022.03.004

Mínguez, A. (2021). Visión por computador e inteligencia artificial: Aplicaciones en la industria 4.0. Revista de Innovación Tecnológica. 18(2), 105–122.

Nuñez, D. (2024). istema de control de acceso mediante reconocimiento facial en instituciones educativas de Cuenca. Revista de Tecnología Aplicada. 9(1), 89–97.

Prince, S. J. (2023). Computer vision: Models, learning, and inference. Cambridge University Press.

Ramírez, A. A., Orellana, L. M., Tapia, R. D., Treves, R. V., & Tisoc, J. H. (2023). MÉTODOS DE INVESTIGACIÓN CIENTÍFICA. Instituto Universitario de Innovación Ciencia y Tecnología Inudi Perú S.A.C.

Ramírez, M., López, A., & Jara, F. (2023). Metodologías aplicadas al desarrollo de sistemas con inteligencia artificial. Revista Científica de Ingeniería. 15(2), 33–45.

Reaño, R., Carrión, P., & Mansilla, J. (2023). Control de acceso mediante reconocimiento facial con redes neuronales para zonas restringidas. 310-318.

Rodríguez, M. (2007). Métodos de investigación en sistemas informáticos. Editorial Alfaomega.

Sampieri, R. H., & Collado, C. F. (2010). Metodología de la investigación (5.ª ed.). McGraw-Hill.

Sánchez, P. (2023). Sistemas ciberfísicos: una revisión de sus aplicaciones y desafíos. Revista Electrónica de Ingeniería. 21(3), 77–92.

SHARC Door Controls Inc. (5 de julio de 2023). SHARC Door Controls Inc. Obtenido de SHARC Door Controls Inc: https://sharc.ca/blog/how-electric-strikes-work-with-automatic-door-systems/#:~:text=Una%20cerradura%20el%C3%A9ctrica%20es%20un,acceso%

20env%C3%ADa%20una%20se%C3%B1al%20el%C3%A9ctrica.

Tameson. (julio de 30 de 2025). Tameson. Obtenido de Tameson: https://tameson.es/pages/rele-control#:~:text=Reles%20De%20Conmutaci%C3%B3n-,Qu%C3%A9%20es%20un%20rel%C3%A9%20de%20control,un%20dispositivo%20de%20alta%20potencia.

Tanenbaum, A. S. (2021). Computer networks (6th ed.). Pearson.

Torres, R. (2010). Técnicas cualitativas en la investigación educativa. Fondo de Cultura Económica.

Tuan, T. Q. (2020). rtificial neural networks in pattern recognition: A comprehensive survey. Journal of Computational Intelligence. 36(4), 411–430.

Vaca, E., & Rivera, S. (2022). Uso de OpenCV y Python en el reconocimiento facial para el control de accesos en Riobamba. Revista de Innovación y Tecnología. 14(1), 51–60.

Vorobioff, J., Cerrotta, S., Morel, N., & Amadio, A. (2022). Inteligencia Artificial y Redes Neuronales: Fundamentos, Ejercicios y Aplicaciones con Python y Matlab. edUTecNe. Obtenido de https://www.researchgate.net/publication/359716455_Inteligencia_Artificial_y_Redes_Neuronales_Fundamentos_Ejercicios_y_Aplicaciones

.