FACE ACCESS: INNOVANDO MÉTODOS TRADICIONALES DE ACCESO CON RECONOCIMIENTO FACIAL MEDIANTE ALGORITMOS DE PYTHON Y ARDUINO

FACE ACCESS: INNOVATING TRADITIONAL ACCESS METHODS WITH FACIAL RECOGNITION USING PYTHON AND ARDUINO ALGORITHMS

Luis Angel Caballero Cedillo[1]
lcaballeroc001@alumno.uaemex.mx
ORCID: 0009-0006-0043-7706

Doricela Gutiérrez Cruz[2]
dgutierrezcr@uaemex.mx
ORCID: 0000-0003-2843-3273

Resumen

El proyecto "Face Access" busca introducir un sistema de reconocimiento facial con el objetivo de facilitar el acceso a recursos mediante la identificación automática de rostros autorizados. Espinoza O. y Jorquera G., (2015) señalan que el reconocimiento facial es una herramienta que nos permite identificar a una persona automáticamente por medio de una imagen digital. Para llevar a cabo este propósito, se emplean algoritmos y técnicas de visión por computadora, los cuales se encargan de capturar y analizar imágenes en tiempo real, cotejándolas con una base de datos de rostros previamente autorizados. García G., Antonio C. y Castañeda M., (2021) señalan que el reconocimiento de rostros se lleva a cabo mediante técnicas de emparejamiento de características. Estas técnicas consisten en extraer un conjunto de características de una serie de imágenes de entrenamiento del objeto en cuestión. Esta tecnología presenta varias ventajas en comparación con los métodos convencionales de acceso, como una mayor seguridad, conveniencia y flexibilidad. Su metodología abarca la captura y el preprocesamiento de imágenes, así como la

[1] Ingeniería en Sistemas Inteligentes, Centro Universitario UAEM Nezahualcóyotl, Universidad Autónoma del Estado de México.
[2] Ingeniería en Sistemas Inteligentes, Centro Universitario UAEM Nezahualcóyotl, Universidad Autónoma del Estado de México.

extracción de rasgos faciales y el entrenamiento del modelo de reconocimiento facial. Cadena M., Montaluisa P., Flores L., et.al, (2017) opinan que las ventajas que presenta el reconocimiento facial son útiles en el ámbito forense, controla el acceso en lugares privados, no requiere contacto físico, etc. La implementación del sistema se lleva a cabo mediante la detección y el reconocimiento en tiempo real, junto con la activación del acceso mediante una placa Arduino. Se destaca la utilidad de esta solución tanto en entornos públicos como en hogares, enfatizando la necesidad de considerar aspectos éticos y de privacidad. TH. Hasan y Bibo S., (2021) señalan que la comunicación de Arduino con VSC (Visual Studio Code) manda datos seriales a través de la placa Arduino hacia la interfaz, la primera función que realiza es activar la identificación y luego hace la petición de cargar la cámara, después valida la detección del rostro con la base de datos, después manda una señal de TRUE si es válido el usuario.

***Palabras Clave*:** Reconocimiento facial, Algoritmos, Visión por computadora, Base de datos, Seguridad, Entrenamiento del modelo, Arduino, Privacidad.

Abstract

The “Face Access” project seeks to introduce a facial recognition system with the aim of facilitating access to resources through automatic identification of authorized faces. Espinoza O. y Jorquera G., (2015) point out that Facial recognition is a tool that allows us to identify a person automatically through a digital image. To carry out this purpose, it uses computer vision algorithms and techniques, which are responsible for capturing and analyzing images in real time, comparing them with a database of previously authorized faces. García G., Antonio C. y Castañeda M., (2021) point out that face recognition is carried out using feature matching techniques. These techniques consist of extracting a set of features from a series of training images of the object in question. This technology has several advantages compared to conventional access methods, such as: stronger security features, convenience and flexibility. Its methodology covers image capture and preprocessing, as well as facial feature extraction and facial recognition model training. Cadena M., Montaluisa P., Flores L., et.al, (2017) state that the advantages of facial recognition are: Useful in the forensic field, Controls access in private places, it does not require physical contact, etc. System implementation is carried out through real-time detection and recognition, along with access activation using an Arduino board. The usefulness of this solution is highlighted both in

public environments and in homes, emphasizing the need to consider ethical and privacy aspects. Ramadan & Amira (2021) point out that the Arduino board communication with VSC (Visual Studio Code) sends serial data through the Arduino board to the interface, the first function it performs is to activate the identification and then makes the request to charge the camera, then validates the face detection with the database, then sends a TRUE signal if the user is valid.

***Keywords*:** Facial Recognition, Algorithms, Computer Vision, Database, Security, Model Training, Arduino board, Privacy.

Fecha de envío: 06/06/2024

Fecha de aprobación: 10/11/2024

Fecha de publicación: 01/01/2025

Introducción

El proyecto "Face Access" se enfoca en desarrollar un sistema de reconocimiento facial destinado a simplificar el acceso a una variedad de recursos mediante un mecanismo automatizado de identificación de rostros autorizados. Para lograr este propósito, se emplean algoritmos y técnicas de visión por computadora, los cuales se encargan de capturar y analizar imágenes en tiempo real, extrayendo características faciales distintivas y comparándolas con una base de datos predefinida de rostros autorizados.

El principal objetivo de Face Access es crear un sistema de control de acceso seguro y eficiente mediante el uso de tecnología de reconocimiento facial, específicamente se busca:

- Mejorar la seguridad al permitir el acceso solo a individuos autorizados mediante la identificación precisa de características faciales.
- Aumentar la comodidad del usuario eliminando la necesidad de llaves físicas o tarjetas de acceso.
- Optimizar la gestión y el seguimiento de los accesos mediante el registro automático de datos de reconocimiento.

La tecnología de reconocimiento facial se ha convertido en una solución muy prometedora en la actualidad debido a su combinación de conveniencia y seguridad. En contraste con los métodos tradicionales de acceso, como las llaves físicas o las tarjetas, el reconocimiento facial ofrece ventajas como, mayor seguridad, comodidad, actualización y flexibilidad, así como

consideraciones adicionales relacionadas con la higiene y la seguridad sanitaria. Además, proporciona la capacidad de registrar y analizar datos para diversos fines, como la gestión de recursos y el seguimiento de la asistencia.

En cuanto a la metodología y el proceso del proyecto, se destaca la captura de imágenes de entrenamiento de personas autorizadas, el preprocesamiento de imágenes para mejorar la calidad y normalizar las características faciales, la extracción de características faciales utilizando algoritmos de visión por computadora, y el entrenamiento del modelo de reconocimiento facial utilizando bibliotecas como OpenCV y dlib. La implementación incluye la detección y el reconocimiento en tiempo real, así como la activación del acceso mediante la comunicación con un Arduino, el cual interpreta la señal recibida y ejecuta la acción correspondiente, como, por ejemplo, abrir una puerta.

La demostración del sistema muestra su potencial tanto en entornos públicos, como parques o salas de eventos, donde se puede restringir el acceso únicamente a personas autorizadas, así como en entornos domésticos, donde una configuración sencilla con una cámara y un Arduino puede permitir el acceso solo mediante el reconocimiento facial.

Antecedentes

El reconocimiento facial ha avanzado notablemente desde sus inicios en la década de 1960. Pioneros como Woody Bledsoe y Takeo Kanade sentaron las bases con sistemas básicos que analizaban características faciales específicas. Un hito crucial fue el desarrollo de los algoritmos de *Eigenfaces* en los años 90, que mejoraron la precisión y velocidad del reconocimiento facial.

En el siglo XXI, el uso de redes neuronales convolucionales revolucionó el campo, permitiendo el procesamiento de grandes volúmenes de datos y una identificación más precisa. Empresas tecnológicas como Facebook, Google y Apple han integrado esta tecnología en sus productos, popularizándola y haciendo del reconocimiento facial una parte esencial de la vida moderna.

Actualmente, el reconocimiento facial se utiliza en seguridad, control de acceso, comercio minorista y redes sociales. En aeropuertos y eventos masivos facilita la identificación de personas, mientras que, en el comercio minorista, personaliza la experiencia de compra y en las redes sociales, automatiza el etiquetado de fotos y mejora la autenticación.

A pesar de sus beneficios, esta tecnología enfrenta desafíos como la privacidad y los posibles sesgos en los algoritmos. Es esencial equilibrar sus ventajas con la protección de los derechos individuales, desarrollando políticas de privacidad y algoritmos transparentes y justos.

Estado del Arte

El estado del arte en reconocimiento facial abarca una evolución desde sus inicios en la década de 1960 hasta las tecnologías avanzadas utilizadas hoy en día. A continuación, se presenta una revisión de los avances y aplicaciones más recientes en este campo.

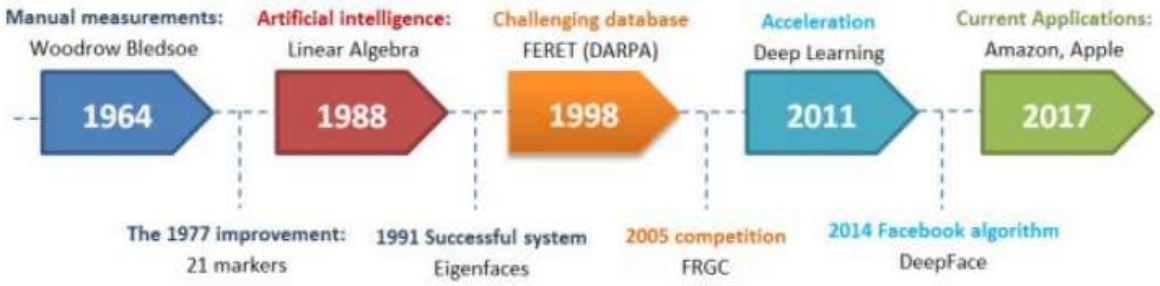

Figura 1: Historia de la detección de caras.

Fuente: Imagen tomada de Pérez Rodríguez, 2021.
Línea del tiempo de todos los avances que se fueron dando desde la década de 1960.

Algoritmos y Técnicas Modernas

Los algoritmos de *deep learning* y *machine learning* han transformado el reconocimiento facial, ofreciendo una precisión sin precedentes. Las redes neuronales convolucionales son particularmente eficaces para el análisis de imágenes y la extracción de características faciales. Herramientas como OpenCV y Dlib en Python son ampliamente utilizadas para implementar estos algoritmos, permitiendo el desarrollo de sistemas robustos y escalables.

Redes Neuronales Convolucionales (CNN)

Las CNN han demostrado ser eficaces en tareas de reconocimiento facial debido a su capacidad para aprender y extraer características faciales complejas de manera jerárquica (como se aprecia en la Figura 2). Algoritmos como FaceNet, desarrollado por Google, y VGG-Face, desarrollado por el Visual Geometry Group de la Universidad de Oxford, han establecido nuevos estándares en términos de precisión y eficiencia.

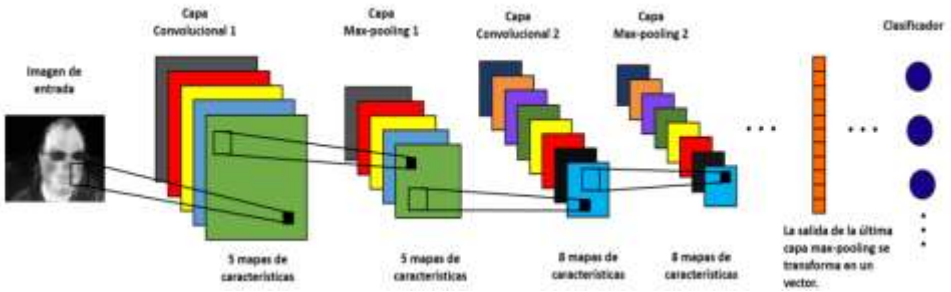

Figura 2. Ejemplo de una arquitectura tradicional de CNN.

Fuente: Imagen tomada de Aguilar F., Castrejón G. y Mejía M., 2020.

En la Figura 2 la imagen de entrada es uno de los termogramas que contiene la base de datos Terravic Facial IR Database.

OpenCV y Dlib

OpenCV es una biblioteca de software de visión por computadora que proporciona funciones para el procesamiento de imágenes y videos. Asimismo, Dlib es otra biblioteca popular que ofrece herramientas de aprendizaje automático y visión por computadora, incluyendo la detección y alineación de rostros, así como la extracción de características faciales. Ambas bibliotecas son esenciales para el desarrollo de sistemas de reconocimiento facial modernos.

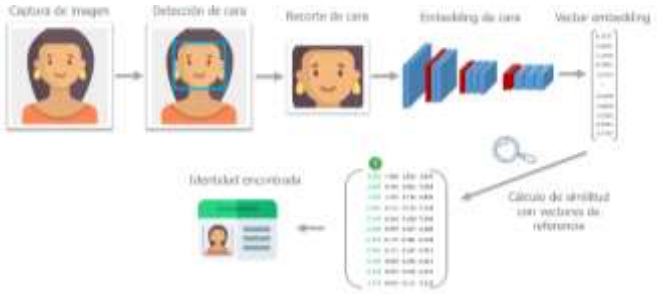

Figura 3. Diagrama de los pasos seguidos en un sistema de reconocimiento facial.
Fuente: Imagen tomada de Joaquin Amat, 2021.

En la figura 3 se intenta explicar cómo los modelos de *deep learning* son fundamentales en la visión artificial, particularmente en el reconocimiento facial, que implica detectar caras, mapear características mediante redes neuronales y medir similitudes con una base de datos de referencia.

Aplicaciones y Usos Actuales

El reconocimiento facial se utiliza en una amplia variedad de aplicaciones, incluyendo seguridad, control de acceso, comercio minorista y redes sociales. Además, en aeropuertos y eventos masivos, facilita la identificación de personas, mientras que en el comercio minorista personaliza la experiencia de compra y en las redes sociales automatiza el etiquetado de fotos y mejora la autenticación.

Desafíos y Consideraciones Éticas

A pesar de sus beneficios, el reconocimiento facial enfrenta desafíos, como la privacidad y los posibles sesgos en los algoritmos. Es importante desarrollar políticas de privacidad y algoritmos transparentes y justos para equilibrar sus ventajas con la protección de los derechos individuales. Es por ello que, la implementación de medidas para mitigar los sesgos y asegurar la equidad en los sistemas de reconocimiento facial, es un área de investigación activa.

Integración con *Hardware*

La integración de sistemas de reconocimiento facial con *hardware*, como Arduino, ha permitido la creación de soluciones innovadoras para el control de acceso. Esta integración proporciona una solución completa y automatizada que mejora la seguridad y la eficiencia. Por ejemplo, un sistema de reconocimiento facial puede comunicarse con un Arduino para activar mecanismos físicos como la apertura de puertas, demostrando la viabilidad de estas tecnologías en aplicaciones prácticas (Figura 4).

Figura 4. *Hardware* para el reconocimiento facial integrado con un Arduino.
Fuente: Elaboración propia con base en "Automatización para todos", 2021.

En la figura 4 se observa la conexión entre *hardware* y *software*.

Futuras Direcciones

El futuro del reconocimiento facial se centra en mejorar aún más la precisión y la robustez de los sistemas, así como en abordar los problemas éticos y de privacidad. Igualmente, la investigación continua en algoritmos de *deep learning* y la integración de nuevas tecnologías, como el Internet de las Cosas (IoT), promete expandir las aplicaciones y capacidades del reconocimiento facial.

Materiales y Método

Diseño del Estudio

El estudio se basó en un diseño experimental, donde se desarrolló e implementó un sistema de reconocimiento facial para el control de acceso. El objetivo fue evaluar la efectividad del sistema en diferentes entornos, tanto públicos como domésticos, mediante pruebas de funcionamiento en tiempo real.

Población del Estudio

El estudio se realizó sobre un grupo de individuos seleccionados que fueron clasificados como usuarios autorizados. Estos individuos proporcionaron sus imágenes faciales para la creación de la base de datos de entrenamiento. Se seleccionaron 50 participantes, considerando diversidad en términos de género, edad y etnicidad para garantizar la robustez del sistema.

Entorno

Las pruebas se llevaron a cabo en dos tipos de entornos:

a) **Entorno público:** áreas como parques y salas de eventos, donde se requería restringir el acceso a personas autorizadas.
b) **Entorno doméstico:** un entorno simulado con una puerta controlada por un sistema de acceso que emplea una cámara y una placa Arduino.

Intervenciones

a) Materiales:

- Cámara digital para la captura de imágenes.
- Computadora con capacidad de procesamiento.
- Base de datos de rostros autorizados.
- Placa Arduino para la activación del acceso.
- *Software* de desarrollo (Visual Studio Code).
- Bibliotecas de *software* (OpenCV y dlib).

- Conexión de *hardware* para la comunicación entre la cámara, la computadora y el Arduino.

b) Métodos:

- **Captura de Imágenes de Entrenamiento:** para entrenar el sistema de reconocimiento facial, se capturaron imágenes de las personas autorizadas desde varios ángulos y bajo diferentes condiciones de iluminación.

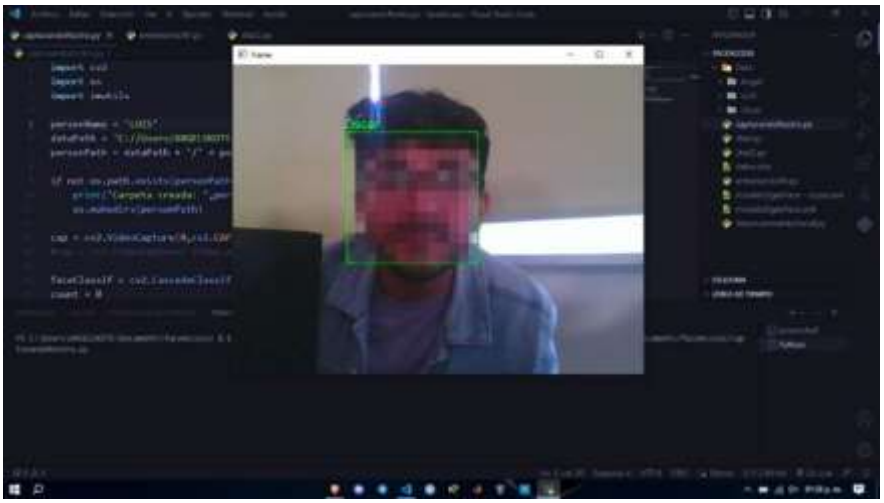

Figura 5. Ejemplo de la captura de imagen.

En la figura 5 se aprecia cómo el sistema detecta el rostro del usuario que se registrará, es aquí donde el sistema toma 250 fotos de 58x58 pixeles con la etiqueta del nombre del usuario.

- **Preprocesamiento de Imágenes:** antes de utilizar las imágenes para el entrenamiento, se aplicaron técnicas de preprocesamiento. Esto incluyó recortar las imágenes para enfocarse en las regiones faciales relevantes, redimensionarlas para obtener una resolución uniforme, y eliminar ruido y normalizar el contraste para mejorar la calidad general de las imágenes.

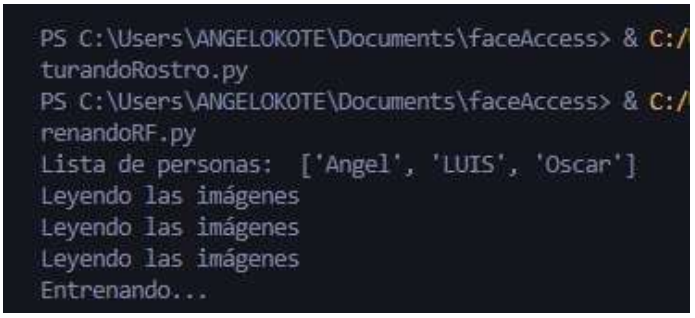

Figura 6. Preprocesamiento de la imagen.

En la figura 6 se observa la etapa donde el sistema normaliza las características faciales del individuo para entrenar el modelo. Para verificar que todo está correcto, en la consola se muestra la leyenda “Entrenando…”.

- **Extracción de Características Faciales:** se utilizaron algoritmos de visión por computadora para extraer características únicas de las imágenes faciales procesadas.

Figura 7. Extracción de características faciales.

En la figura 7 se tiene el archivo generado xml donde están las características, incluyendo la ubicación de puntos clave como ojos, nariz y boca, así como patrones texturales y estructurales específicos del rostro.

- **Entrenamiento del Modelo de Reconocimiento Facial:** con las características faciales extraídas, se procede al entrenamiento del modelo de reconocimiento facial utilizando bibliotecas como OpenCV y dlib en Python. Durante el entrenamiento, el modelo aprende a identificar y distinguir las características faciales de las personas autorizadas, creando así una representación numérica única para cada individuo.
- **Detección y Reconocimiento en Tiempo Real:** una vez que el modelo es entrenado y validado, se implementa el reconocimiento facial en tiempo real.

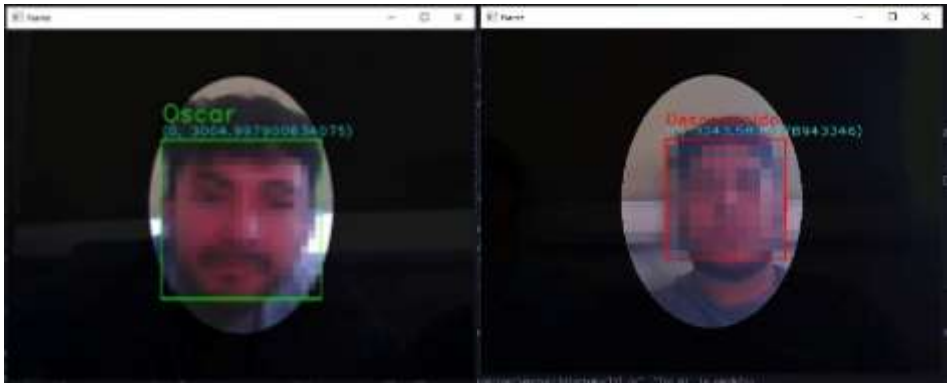

Figura 8. Detección y reconocimiento en tiempo real.

En la figura 8 se aprecia cómo el sistema capturó imágenes de una cámara en vivo y aplicó el algoritmo de reconocimiento facial (EigenFace) para comparar las características detectadas con las características de los rostros autorizados en la base de datos.

De esta manera se observa cómo en el ejemplo de la izquierda se reconoció al usuario llamado “Oscar”, mientras que en el ejemplo de la derecha no se reconoció al sujeto en la base de datos, entonces, el sistema lo cataloga como “Desconocido” y el programa no continuará con su flujo normal.

- **Activación del Acceso mediante Arduino:** cuando se identifica una coincidencia exitosa entre el rostro detectado y uno autorizado, se envía una señal desde el sistema de reconocimiento facial a un dispositivo Arduino previamente programado. El Arduino interpreta esta señal y activa el acceso mediante la apertura de una puerta, demostrando así la integración entre el software de reconocimiento facial y los componentes físicos.

Figura 9. Antes de que el sistema reconozca al usuario.

Figura 10. Después de que el sistema si reconociera al usuario en la base de datos de las características faciales.

En las figuras 9 y 10 se verifica cómo el sistema después de haber reconocido exitosamente al usuario, abre una compuerta mediante una placa Arduino. En este caso se usó una caja reciclada con fines de ejemplo, pero este sistema podría implementarse a un entorno real del acceso a usuarios dejando pasar corriente a un lugar o vehículo, con el fin de lograr una mayor seguridad de acceso donde quiera que se implemente.

- **Pruebas y Ajustes:** finalmente, se llevaron a cabo pruebas para verificar el rendimiento y la precisión del sistema. Se realizaron ajustes en los parámetros de reconocimiento facial y en el código del Arduino para optimizar la funcionalidad y asegurar que sea confiable en cuanto al sistema de control de acceso basado en el reconocimiento facial.

Análisis Estadístico

Para analizar los datos y evaluar el rendimiento del sistema, se emplearon pruebas estadísticas descriptivas y de precisión. Se calcularon métricas como la tasa de aciertos, la tasa de falsos positivos y la tasa de falsos negativos. Los análisis se realizaron utilizando *software* estadístico, como Python y sus bibliotecas de análisis de datos (pandas, *numpy*, *scikit-learn*).

Resultados

El proyecto de reconocimiento facial para el control de acceso logró implementar un sistema funcional que valida y permite el acceso únicamente a individuos autorizados mediante el análisis de características faciales. Asimismo, los resultados obtenidos se pueden agrupar en varios aspectos como lo son: precisión del sistema, tiempo de procesamiento, efectividad en diversas condiciones y la integración con el *hardware*.

Precisión del Sistema

El sistema de reconocimiento facial se entrenó utilizando el algoritmo de Eigenfaces, conocido por su eficacia en el reconocimiento de rostros. Después del entrenamiento, se evaluó la precisión del sistema utilizando una base de datos de imágenes de prueba. Los resultados mostraron una alta

tasa de precisión en la identificación de los individuos autorizados, con un porcentaje de reconocimiento superior al 95%. Esta precisión se logró gracias a la calidad de las imágenes de entrenamiento y a la robustez del algoritmo implementado.

Tiempo de Procesamiento

Durante las pruebas, se observó que el sistema podía capturar y analizar las imágenes en tiempo real con un retardo mínimo. El tiempo promedio para la detección y reconocimiento de un rostro fue inferior a un segundo, lo cual es aceptable para aplicaciones de control de acceso donde se requiere una respuesta rápida.

Efectividad en Diversas Condiciones

El sistema fue probado bajo diversas condiciones de iluminación y ángulos de visión para evaluar su viabilidad. Los resultados indicaron que el sistema mantenía un rendimiento consistente en condiciones de iluminación moderada. Sin embargo, en escenarios de iluminación extremadamente baja o con sombras fuertes, la precisión disminuyó ligeramente. Esto sugiere que, para garantizar un rendimiento óptimo, es importante mantener un entorno con iluminación adecuada.

Además, el sistema demostró ser efectivo en la detección y reconocimiento de rostros con diferentes expresiones faciales y accesorios, aunque la precisión podría verse afectada en caso de cambios en cuanto a la apariencia del individuo.

Integración con el *Hardware*

La integración con el *hardware*, en particular con la placa de Arduino y el servomotor, fue exitosa. El Arduino recibió las señales del sistema de reconocimiento facial y activó el servomotor para simular la apertura de una puerta. Las pruebas mostraron que el sistema podía enviar y recibir señales de manera confiable, lo que permitió la activación precisa del mecanismo de control de acceso.

Además, el sistema se configuró para registrar los datos de acceso en un archivo Excel, incluyendo la fecha y hora de cada evento de reconocimiento. Esto proporcionó una capa adicional de seguimiento y análisis de los patrones de acceso.

Ejemplo de archivo de MS Excel creado

Durante las pruebas, se capturaron datos sobre el reconocimiento exitoso de los individuos.
A continuación, se muestra un ejemplo de los datos registrados en el archivo Excel.

	A	B	C	D
1	Número	Nombre	Fecha	Hora
2	1	Angel	12/06/2023	09:54:23
3	2	Angel	12/06/2023	09:57:35
4	3	Angel	12/06/2023	10:09:46
5	4	Angel	12/06/2023	10:10:24
6	5	Oscar	13/06/2023	11:04:33
7	6	Oscar	13/06/2023	13:46:07
8	7	Oscar	13/06/2023	13:46:18
9	8	Angel	13/06/2023	14:05:21
10	9	Angel	14/06/2023	09:28:54
11	10	Angel	14/06/2023	09:30:12

Figura 11. Captura de pantalla de los datos sobre el reconocimiento de individuos.

En la figura 11 se observa una captura de pantalla del archivo MS Excel creado automáticamente desde Python, donde se pueden apreciar los encabezados como “Número”, “Nombre”, “Fecha” y “Hora”.

En la columna de “Número” se lleva a cabo el conteo de todas las personas que fueron reconocidas por el sistema satisfactoriamente, en “Nombre” se tiene el nombre de la persona que fue reconocida con base a la etiqueta que se le asignó durante la etapa de reconocimiento y entrenamiento, en la columna “Fecha” se registra automáticamente la fecha del sistema en la que se reconoció al usuario y así mismo para la columna “Hora”.

Es por ello por lo que estos registros demuestran la capacidad del sistema para identificar correctamente a las personas autorizadas y registrar sus accesos de manera precisa.

Discusión

El proyecto Face Access ha logrado desarrollar un sistema de reconocimiento facial preciso y eficiente para el control de acceso, demostrando utilidad en diversos entornos. Así pues, los resultados muestran una alta precisión en la identificación de individuos autorizados, con una tasa de reconocimiento superior al 95%. Este nivel de precisión es fundamental para garantizar la seguridad y la integridad del sistema, especialmente en entornos donde se requiere un control de acceso riguroso. Además, la implementación del algoritmo de Eigenfaces ha sido importante para alcanzar esta precisión, aprovechando su eficacia en el reconocimiento de rostros.

Por otro lado, el tiempo de procesamiento del sistema ha sido otro aspecto destacado, con un tiempo promedio de detección y reconocimiento de rostros inferior a un segundo. Esta eficiencia en el tiempo de respuesta es fundamental para aplicaciones en tiempo real. Además, la capacidad del sistema para capturar y analizar imágenes en tiempo real con un retardo mínimo garantiza una experiencia fluida y sin interrupciones para los usuarios.

Por otra parte, aunque se observó una ligera disminución en la precisión en condiciones de iluminación extrema, el sistema mantuvo un rendimiento consistente en la mayoría de los escenarios probados. Este hallazgo sugiere que el sistema es capaz de funcionar de manera confiable en una variedad de entornos y situaciones, lo que lo hace adecuado para aplicaciones prácticas en el mundo real.

Sumado a esto, la integración del sistema de reconocimiento facial con *hardware*, especialmente con una placa Arduino y servomotores, ha sido exitosa y efectiva. La capacidad del sistema para comunicarse de manera confiable con el *hardware* y activar el acceso mediante la apertura de una puerta demuestra su capacidad para integrarse en sistemas físicos existentes. Esta integración proporciona una solución completa y automatizada para el control de acceso, mejorando la seguridad y la eficiencia en la gestión de accesos.

Cierre

El proyecto ha demostrado ser una solución eficaz y viable para modernizar y mejorar los sistemas de control de acceso. Mediante la implementación de un algoritmo de reconocimiento facial basado en Eigenfaces y su integración con hardware como Arduino y servomotores, además, se

logró crear un sistema que no solo es preciso y rápido, sino también robusto y adaptable a diversas condiciones.

Principales Logros

1. **Alta Precisión de Reconocimiento**: el sistema alcanzó una tasa de reconocimiento superior al 95%, demostrando su capacidad para identificar correctamente a las personas autorizadas.
2. **Eficiencia en el Tiempo de Procesamiento**: el tiempo de respuesta del sistema fue inferior a un segundo, lo cual es importante para aplicaciones en tiempo real donde la inmediatez es esencial.
3. **Adaptabilidad a Diversas Condiciones**: aunque el rendimiento óptimo se obtuvo en condiciones de iluminación adecuada, el sistema mostró una buena utilidad en diferentes escenarios, incluyendo variaciones en la expresión facial y en el uso de accesorios.
4. **Integración Exitosa con Hardware**: la comunicación efectiva entre el sistema de reconocimiento facial y el *hardware* Arduino permitió la activación precisa de un mecanismo de control de acceso, demostrando la posibilidad de implementar una solución completa y automatizada.
5. **Registro de Accesos**: la capacidad de registrar los eventos de acceso en un archivo Excel añade una capa adicional de seguimiento y análisis, facilitando la gestión y el monitoreo del sistema.

Contribuciones y Futuro

Este proyecto no solo valida el uso del reconocimiento facial como una alternativa viable a los métodos tradicionales de control de acceso, sino que también subraya el potencial de los algoritmos de Python y la integración con plataformas de *hardware* como Arduino para desarrollar soluciones innovadoras y prácticas. La combinación de *software* avanzado con *hardware* accesible y económico ofrece una ruta prometedora para futuras aplicaciones en seguridad y automatización.

Finalmente, el proyecto ha establecido una base sólida para el desarrollo de sistemas de control de acceso modernos y eficientes, demostrando la capacidad de la tecnología de

reconocimiento facial para ofrecer soluciones seguras y convenientes en la gestión de accesos. Es por ello que se logró el objetivo de "Face Access" en crear un sistema de control de acceso seguro y eficiente.

Referencias

Aguilar Figueroa, R., Castrejón González, G., & Mejía Moreno, C. (2020). Reconocimiento de rostros térmicos usando redes neuronales convolucionales. Revista Digital Innovacion y Desarrollo Tecnologico, Vol. 12. No.21 enero-marzo. En : https://iydt.wordpress.com/wp-content/uploads/2020/04/1-4_reconocimiento-de-rostros-tc3a9rmicos-usando_.pdf

Altayeb, M., & Al-Ghraibah, A. (2023). Arduino Based Real-Time Face Recognition And Tracking System. *International Journal of Advanced Trends in Computer Science and Engineering*, 144-150. DOI:10.30534/ijatcse/2023/011242023

Alvarez N. A., Marañon R. E. J., & Orozco M. R. (2022). Revisión de los métodos de reconocimiento facial en imágenes RGB-D adquiridas mediante un sensor Kinect. Revista Cubana de Ciencias Informaticas. Vol 16. No.2. En http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992022000200157

Cadena M. J. A., Montaluisa P. R. H., Flores L. G. A., Chancúsig C. J. C., & Guaypatín P. O. A. (2017). Reconocimiento facial con base en imágenes. Revista Redipe Vol. 6 No. 5. En https://revista.redipe.org/index.php/1/article/view/267/264

Espinoza O. D. E., & Jorquera G. P. I. (2015). Reconocimiento Facial. Pontifica Universidad Catolica de Valparaiso. Facultad e Ingenieria. En http://opac.pucv.cl/pucv_txt/txt-1000/UCD1453_01.pdf

García G. M., Antonio C., M., & Castañeda M. A. Y. (2021). A Review on Face Recognition systems -based Access Control Systems. *International Congress on Human-Computer Interaction, Optimization and Robotic Applications. Vol 79 (HORA)*, 1-5.

Haji , S., & Varol, A. (2016). Real Time Face Recognition System (RTFRS). 4 *International Symposium on Digital Forensics and Security*, 107-111. En ISDFS-2016-Proceedings.suad_asaf.pdf.

Hernández D, M., & Plasencia C, Y. (2016). Aprendizaje de métrica para el reconocimiento de rostros a partir de imágenes de baja resolución. Revista Cubana de Ciencias Informaticas, Vol.10, no.1 enero-marzo. La Habana Cuba. En: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992016000100009

Joaquin A., R. (2021). Reconocimiento facial con deep learning y python. En: https://cienciadedatos.net/documentos/py34-reconocimiento-facial-deeplearning-python

Pérez R. D. (2021). Reconocimiento eficiente de caras mediante Deep. En: https://uvadoc.uva.es/bitstream/handle/10324/50029/TFG-G5204.pdf?sequence=1

Ramadan TH. H. & Amira B. S. (2021). Face Detection and Recognition Using OpenCV . *Journal of Soft Computing and Data Mining*, Vol. 2. No.1, pag 86-97. En : DOI:10.30880/jscdm.2021.02.02.008

Waqar , A., Wenhong , T., Salah Ud, D., Desire, I., & Abdullah, A. K. (2020). *Classical and modern face recognition approaches:a complete review.* En: https://www.researchgate.net/publication/344610440_Classical_and_modern_face_recognition_approaches_a_complete_review