RECONOCIMIENTO FACIAL PARA CONTROL DE ACCESO

Conference Proceedings ICONIS – VIII 2024.
Mazatlán, México, Mayo 29-31, 2024. Pag. 195-200

ISSN (Online): 2711-3310

Alejandro, Jacinto Lucas*	**David, Luviano Cruz**	**Luz Angelica, García Villalba**	**Diana Yaziel, Ortiz Muñoz**	**Luis Asunción, Pérez Domínguez**
Universidad Autónoma de Ciudad Juárez. Departamento de ingeniería industrial y manufactura. Al7999@alumnos.uacj.mx	*Universidad Autónoma de Ciudad Juárez. Departamento de ingeniería industrial y manufactura. David.luviano@uacj.mx*	*Universidad Autónoma de Ciudad Juárez. Departamento de ingeniería industrial y manufactura. lugarcia@uacj.mx*	*Universidad Autónoma de Ciudad Juárez. Departamento de ingeniería industrial y manufactura. Diana.ortiz@uacj.mx*	*Universidad Autónoma de Ciudad Juárez. Departamento de ingeniería industrial y manufactura. Luis.dominguez@uacj.mx*

Resumen: ***El proyecto se centra en el desarrollo de un algoritmo de reconocimiento facial en Python que emplea detección de rostros y reconocimiento facial mediante redes neuronales convolucionales. Su propósito es mejorar el acceso a viviendas mediante una cerradura electrónica, ofreciendo una alternativa segura y avanzada a métodos tradicionales. La integración de tecnologías modernas con un mecanismo físico de seguridad busca reducir robos y acceso a propiedades privadas, fortaleciendo la autenticación basada en biometría facial para mejorar la seguridad del hogar.***

Palabras clave: Haarcascade, Red neuronal convolucional, Reconocimiento facial.

1 INTRODUCCIÓN

La seguridad en el acceso a datos, recursos e instalaciones es fundamental en la actualidad basándose en los principios clave de la identificación. Autentificación y

* Citación: Jacinto Lucas, A., Luviano Cruz, D., García Villalba, L. A., Ortiz Muñoz, D. Y. y Pérez Domínguez, L. A. (2024). Reconocimiento facial para control de acceso. *Conference Proceedings of the International Congress on Innovation and Sustainable*, Mazatlán, México, Mayo 29-31, 2024, p.p. 195–200.

autorización del usuario. En este contexto la biometría surge como un enfoque innovador, aprovechando las características físicas únicas de las personas, como las huellas dactilares o el reconocimiento facial. Este último, ha cobrado relevancia en diversos ámbitos, desde el desbloqueo de dispositivos hasta el control de acceso en aeropuertos.

En México, donde la seguridad es una preocupación constante, se observa un alto índice de delitos no denunciados en cuanto a robo a casa habitación. (Central de Alarmas de México, 2023). Ante esta problemática, el acceso tradicional con llaves, códigos o tarjetas de acceso presenta vulnerabilidades de robo, olvido u extravió. Tomando eso en cuenta, se propone un sistema de reconocimiento facial basado en redes neuronales convolucionales, aplicado en el control de acceso a una casa habitación, que ofrece una alternativa segura y conveniente, reduciendo el riesgo de acceso no autorizado y simplificando el proceso de acceso a los usuarios. El presente proyecto tiene fines académicos, promoviendo la seguridad y la salud al evitar el contacto con dispositivos de autenticación compartidos.

2 MARCO TEÓRICO Y CONCEPTUAL

- **Biometría.**

La biometría es la ciencia del reconocimiento de individuos basándose en las características únicas de cada persona. (kaspersky, 2024) Se trata de un proceso similar al que realiza el ser humano identificado personas por medio de su aspecto físico, su voz, o su forma de caminar.

- **Reconocimiento facial.**

El reconocimiento facial es un método de autenticación mediante características faciales, se logra combinando dos áreas de inteligencia artificial: visión por computadora y aprendizaje profundo. Su funcionamiento se basa en comparar características faciales de un rostro detectado con un conjunto de imágenes de rostros ya registrados anteriormente en una base de datos,

evaluando la coincidencia que hay entre estas. (Bansal, Agarwal, Sharma, & Gupta, 2013)

- **Haarcascade.**

Este algoritmo utiliza conjuntos de imágenes con rostros y sin rostros para entrenar un clasificador. Utiliza funciones de Haar para extraer características faciales. Las imágenes integrales ayudan a manejar la gran cantidad de características, posterior-mente, Adaboost selecciona características relevantes. El proceso de selección de características aplica cada función al conjunto de imágenes de entrenamiento buscando el mejor umbral para distinguir entre rostros y no rostros. Finalmente, se emplea una cascada de clasificadores concentrándose en las regiones más propensas a contener un rostro. (Sriratana, Mukma, Tammarugwattana, & Sirisantisamrid, 2018)

- **Rede neuronal convolucional (CNN).**

Las redes neuronales convolucionales son una variante de las redes neuronales artificiales, inspiradas en el procesamiento visual del cerebro humano, son efectivas en la identificación de patrones en imágenes. Las 3 principales características de CNN son:

Las capas convolucionales emplean filtros para analizar la entrada, identificando patrones como limites, tonalidades o texturas.

Las capas de agrupación disminuyen la cantidad de parámetros en la red, preservando las características más importantes.

Finalmente, las capaz totalmente conectadas vinculan todas las neuronas de la capa precedente, posibilitando la ejecución de clasificaciones definitivas. (Tao, He, & Chen, 2019)

3 METODOLOGÍA

Se recolectaron 3,000 imágenes de entrenamiento y 600 de validación de rostros de 3 usuarios por medio de archivos de video, cada usuario contribuyo con 1000 imágenes de entrenamiento y 200 de validación. Los videos se grabaron desde

diferentes ángulos e iluminaciones. Posteriormente, se desarrolló un algoritmo en Python utilizando Haarcascade para detectar y enmarcar los rostros detectados en los videos generando capturas de NxN pixeles, mismas que se utilizaron para el entrenamiento de la CNN.

La red neuronal convolucional se entrenó con tres capas convolucionales y tres de agrupación, para extraer y clasificar características. El algoritmo de reconocimiento facial cargara el modelo entrenado, capturara video desde una cámara web, detectara rostros en cada cuadro, preprocesara las imágenes faciales y realizara la predicción.

Durante la identificación, la CNN analiza la región facial de cada rostro detectado, mostrando el nombre de la persona y enmarcando su rostro en verde si la probabilidad supera un umbral establecido. En caso contrario, se muestra "Desconocido" y se enmarca el rostro en rojo.

Además, se implementó una cerradura electrónica que se activa mediante Arduino si el rostro detectado se reconoce con éxito, permaneciendo cerrada en caso contrario.

4 RESULTADOS

Se probo en 20 imágenes, 7 videos y 3 grabaciones mediante la cámara web para observar la efectividad del algoritmo de detección de rostros, tal como se muestra en Ilustración 1.

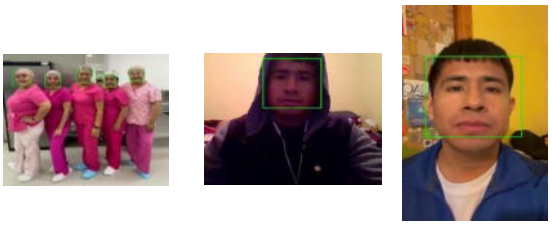

ILUSTRACIÓN 1. DETECCIÓN DE ROSTROS EN IMAGEN, CÁMARA WEB Y ARCHIVO DE VIDEO.

El cálculo de porcentaje de precisión se obtuvo mediante la formula:

$$\frac{Detecciones\ correctas}{Detecciones\ correctas\ +\ Detecciones\ incorrectas} \times 100$$

Logrando una precisión del 88.57%.

La arquitectura de la base de datos de usuarios reconocibles se muestra en Ilustración 2. Además, Ilustración 3 presenta ejemplos de imágenes de rostros recopiladas.

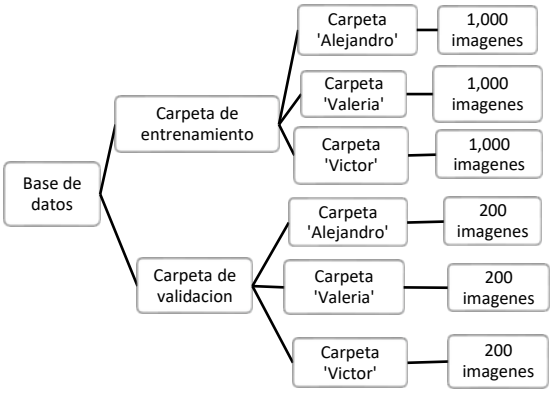

ILUSTRACIÓN 2. BASE DE DATOS

ILUSTRACIÓN 3. IMÁGENES DE ENTRENAMIENTO

Finalmente, la ilustración 4 muestra cómo cambia la precisión de la CNN durante el entrenamiento. La precisión alcanza alrededor del 97% en entrenamiento y 85% en validación.

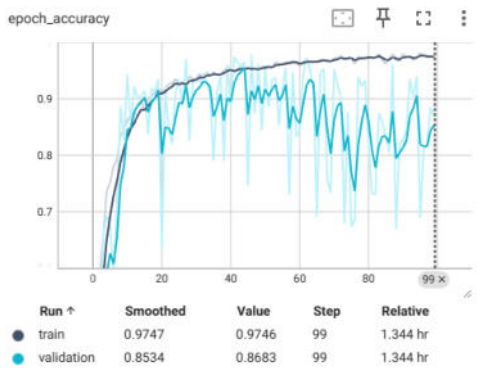

ILUSTRACIÓN 4. GRAFICA DE PERDIDA Y PRECISIÓN A LO LARGO DEL ENTRENAMIENTO DE LA CNN.

Finalmente, la ilustración 5 muestra los resultados del modelo de clasificación mediante la matriz de confusión.

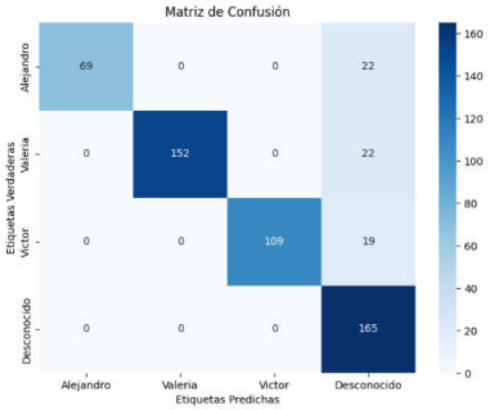

ILUSTRACIÓN 5. MATRIZ DE CONFUSIÓN DE LA CNN.

Se observa que la mayoría de las confusiones son catalogadas como "desconocido". Las ocasiones en las que el sistema confunde entre las etiquetas "Alejandro", "Valeria" y "Víctor" presenta riesgos menores de falsos positivos.

5 CONCLUSIONES

En este proyecto, se ha diseñado un sistema de reconocimiento facial con Python y Arduino, alcanzando una precisión del 88.7% en la identificación de usuarios. Los resultados demuestran la capacidad

del sistema como solución para fortalecer la seguridad y la eficacia en el control de acceso. Futuras mejoras comprenden el desarrollo de una interfaz gráfica y a gestión de una base de datos para el registro de accesos con fechas y horarios. Esta implementación destaca la coordinación y relación entre disciplinas como ingeniería mecatrónica, sistemas, software y eléctrica, evidenciando el potencial colaborativo en proyectos interdisciplinarios por un fin común.

6 REFERENCIAS

Bansal, A., Agarwal, M., Sharma, A., & Gupta, A. (2013). A Review Paper on FACIAL RECOGNITION. International Journal on Recent and Innovation Trends in Computing and Communication , 224-228.

Central de Alarmas de México. (18 de Octubre de 2023). Linkedin. Obtenido de Linkedin: https://www.linkedin.com/pulse/la-inseguridad-y-el-robo-casa-habitaci%C3%B3n/?originalSubdomain=es

kaspersky. (29 de Marzo de 2024). kaspersky.com. Obtenido de kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/biometrics

Sriratana, W., Mukma, S., Tammarugwattana, N., & Sirisantisamrid. (2018). Application of the OpenCV-Python for Personal Identifier Statement. IEEE.

Tao, K., He, Y., & Chen, C. (2019). Design of Face Recognition System Based on Convolutional Neurak Network. IEEE.