

FaceNet

María de Lourdes Salinas Callejas
Ing. Mecatrónica
Tecnológico de Estudios Superiores de
Cuautitlán Izcalli
Cuautitlán Izcalli , Estado de México
maria.sc@cuautitlan.tecnm.mx
0000-0001-8930-9968

Carlos Antonio Sánchez
Ing. Mecatrónica
Tecnológico de Estudios Superiores de
Cuautitlán Izcalli
Cuautitlán Izcalli , Estado de México
193113128@cuautitlan.tecnm.mx

Oscar Olivares López
Ing. Sistemas Computacionales
Tecnológico de Estudios Superiores de
Cuautitlán Izcalli
Cuautitlán Izcalli , Estado de México
oscar.ol@cuautitlan.tecnm.mx

Resumen— El reconocimiento facial es una tecnología avanzada que utiliza algoritmos de inteligencia artificial y aprendizaje automático para identificar y verificar la identidad de una persona a partir de su rostro, el prototipo FaceNet es un sistema con reconocimiento facial para mejorar la seguridad y la eficiencia en el control de acceso y la autenticación de usuarios en una empresa.

Palabras clave— Reconocimiento facial, redes neuronales, producción, acceso, seguridad

I. INTRODUCCIÓN

La aplicación propuesta consiste en un sistema de reconocimiento facial para registrar de manera automática la entrada y salida de los trabajadores, así como los tiempos muertos por ausencias durante la jornada laboral. Con ello se busca sustituir el registro manual en hojas, que actualmente permite irregularidades en los horarios y falta de control en las salidas intermedias.

El objetivo es mejorar la productividad de las empresas, ya que la falta de control ocasiona reducciones significativas en la producción diaria, afectando la entrega final proyectada en los planes de trabajo y metas a alcanzar.

El sistema facial por medio de la IA “FaceNet”, tiene como finalidad asegurar un seguimiento preciso del cumplimiento de los turnos y reducir tiempo muerto ocasionado por retrasos en las reincorporaciones de los trabajadores a su área de trabajo.

II. ANTECEDENTES

Su origen fue en 1960 creado por Woodrow Wilson, conocido como el pionero de la tecnología, el trabajo en un sistema para clasificar los rasgos del rostro humano a través de la tabla RAND. Ver figura 1.



Fig. 1 Trazos faciales

Su sistema analizaba fotografías y calculaba la distancia entre los ojos, nariz o boca de las personas de forma precisa, pero este procedimiento era aún manual.

A medida que avanzaron las investigaciones en inteligencia artificial y visión por computadora, el reconocimiento facial comenzó a ganar interés en la comunidad científica, aunque seguía siendo limitado por la tecnología disponible. Actualmente, la expresión de reconocimiento facial alude a la inteligencia artificial que permite detectar rostros humanos.

A. Definición y funcionamiento de una interfaz de reconocimiento facial

Una interfaz de reconocimiento facial, es un sistema que utiliza tecnología avanzada para identificar o verificar la identidad de una persona basándose en las características de su rostro. Este tipo de interfaz ocupa algoritmos de procesamiento de imágenes y bases de datos para analizar patrones faciales. El objetivo principal es que permita la identificación segura de usuarios, optimizando el control de acceso y el registro de asistencia del personal.

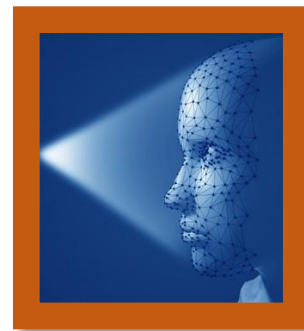


Fig. 2 Reconocimiento facial

La cámara se activa cuando detecta movimiento activando su luz, para poder detectar mejor a la persona y poder tomar su autenticación biométrica del rostro de una persona, el algoritmo detecta el rostro e identifica las características generales del rostro humano, como forma de cara, ojos, nariz y boca, aislando del resto de la imagen. Como se observa en la imagen 2.

B. Procesamiento de imagen

Posteriormente a la identificación del rostro que detecta, la interfaz realiza ajustes para que la imagen sea adecuada para su análisis:

- Alineación: ajusta al rostro para que este orientado correctamente.
- Escalonado: Cambia tamaño de la imagen.
- Filtrado: Elimina imperfecciones o ruido en la imagen, permitiendo que el rostro sea claro y preciso.

Como se observa en la Figura 3 del procesamiento de imagen.



Fig. 3 Procesamiento de imagen

C. Clasificación de reconocimiento

Existen diferentes tipos de interfaces de reconocimiento facial. Cada interfaz tiene sus características específicas, que varían de acuerdo a la tecnología utilizada y el propósito de su implementación.

a) Reconocimiento facial 2D

Analiza las imágenes planas del rostro usando cámaras convencionales.

Depende de la iluminación y el Angulo de la imagen.

- Ventajas: Facilidad de integración en sistemas comunes.
- Desventajas: Más susceptible a errores por cambios de iluminación.

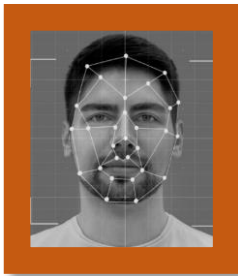


Fig. 4 Reconocimiento facial 2D

b) Reconocimiento facial 3D

Usa sensores de profundidad o cámaras especiales para captar la geometría tridimensional del rostro.

- Ventajas: Mayor precisión, menos afectado por cambios de iluminación y ángulos.
- Desventajas: Requiere equipos más avanzados.



Fig. 5 Reconocimiento facial 3D

c) Reconocimiento facial con Infrarrojo

Usa cámaras infrarrojas para detectar el patrón térmico de los rostros, estas cámaras se basan en el calor emitido por el rostro.

- Ventajas: Funcionan bien en condiciones con poca luz, cambios de accesorios.
- Desventajas: equipos más especializados y sensibles a cambios de temperatura ambiental.

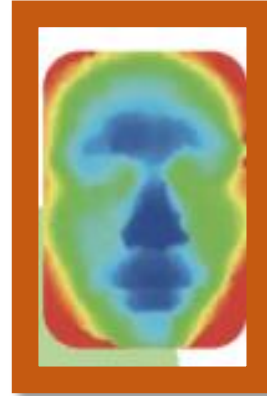


Fig. 1 Reconocimiento facial con infrarrojo

d) Reconocimiento facial basado en puntos clave

Se centran en la identidad de puntos específicos y utilizan algoritmos que comparan la disposición de estos puntos entre diferentes imágenes.

- Ventajas: Mayor velocidad de proceso.
- Desventaja: Puede ser menos preciso en situaciones de poca luz.

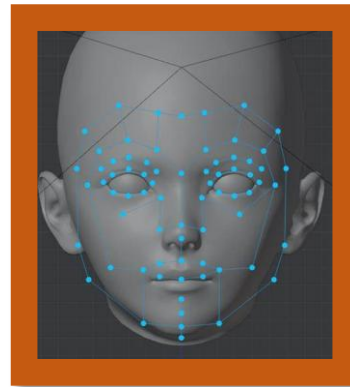


Fig. 7 Reconocimiento facial basado en puntos clave

e) Reconocimiento facial basado en redes neuronales

Usa aprendizaje profundo (Deep learning) para mejora la precisión mediante el análisis de grandes cantidades de datos faciales.

- Ventajas: Alta precisión, adaptabilidad y mejora continua a medida que se entrenan más datos.

- Desventajas: Requiere mucha potencia computacional y gran cantidad de datos para entrenar los modelos.

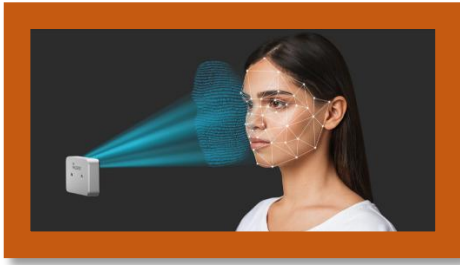


Fig. 8 Reconocimiento facial basado en redes neuronales

f) Reconocimiento facial en tiempo real

Integrado en sistemas de video vigilancia, estos sistemas identifican rostros en tiempo real, a medida que las personas pasan frente a la cámara.

- Ventajas: Monitoreo constante y detección instantánea.
- Desventajas: Grandes cantidades de datos deben ser procesadas rápidamente, lo que puede requerir sistemas robustos.



Fig. 9 Reconocimiento facial en tiempo real

g) Reconocimiento facial en la nube

Procesa imágenes y realiza el reconocimiento facial mediante servicios en la nube.

- Ventajas: Flexibilidad y escalabilidad, no requiere equipos costosos.
- Desventajas: Depende de la conectividad y la seguridad en la transmisión de datos.



Fig. 10 Reconocimiento facial en la nube

El reconocimiento facial ha alcanzado niveles de precisión y eficiencia notables gracias a avances en inteligencia artificial, hardware, y bases de datos más diversas, algunas de sus características actuales son:

Algoritmos dominantes:

- Modelos de Deep Learning más avanzados, como ArcFace, VGGFace2, y Dlib.
- Redes neuronales convolucionales (CNNs) y enfoques basados en transformers, como los utilizados en OpenAI.

Precisión:

- En bases de datos controladas, las tasas de error han bajado al 0.1-0.3%.
- Mayor robustez frente a cambios de pose, iluminación y diversidad étnica gracias a datos de entrenamiento más representativos.

Hardware:

- Cámaras con sensores infrarrojos y ToF (Time of Flight) son comunes en dispositivos móviles.
- Procesadores optimizados para AI en dispositivos de consumo, como los Neural Engines en chips Apple o Tensor Processing Units (TPUs) en teléfonos Android.

Aplicaciones:

- Pagos biométricos: Sistemas como Alipay y Amazon One permiten realizar pagos utilizando el rostro.
- Vigilancia masiva: Integración con cámaras de seguridad y sistemas de análisis en tiempo real.

h) Algoritmo de reducción de dimensiones

Análisis de componentes principales (PCA), su funcionamiento es reducir los datos faciales complejos en representaciones donde se requiera que sean más manejables.

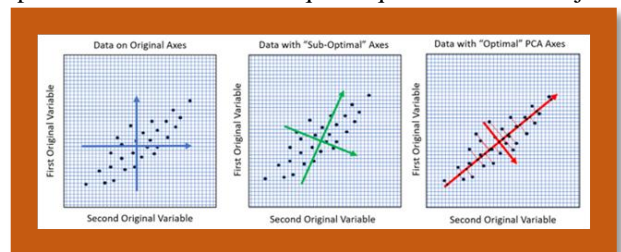


Fig. 11 Algoritmo de reducción de dimensiones

i) Redes neuronales convolucionales (CNN)

Están diseñadas para analizar imágenes y son fundamentales para el reconocimiento facial moderno, proporcionando alta precisión al identificar patrones faciales.

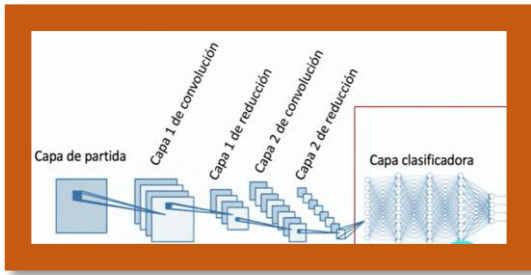


Fig. 12 Redes neuronales convolucionales (CNN)

No obstante, es necesario tener consideraciones que, aunque los algoritmos de reconocimiento facial han mejorado significativamente en los últimos años todavía presentan ciertas limitaciones y desafíos que es importante tener en cuenta:

1. Variabilidad en las condiciones de captura:

Los algoritmos de reconocimiento facial pueden ser sensibles a las variaciones en las condiciones de captura, como iluminación, ángulo de la cara, expresión facial y fondo.

Estas variaciones pueden afectar la precisión del reconocimiento.

2. Cambios en el aspecto:

Los cambios en el aspecto de una persona, como maquillaje, peinado, uso de anteojos o envejecimiento, pueden dificultar la identificación precisa.

3. Datos insuficientes:

Para obtener un rendimiento óptimo, los algoritmos de reconocimiento facial requieren un conjunto de datos amplios y diversos para el entrenamiento (Datasets). Si el conjunto de datos es limitado o sesgado, el reconocimiento puede ser menos preciso.

4. Diferencias étnicas y culturales:

Algunos algoritmos pueden tener dificultades para reconocer rostros de diferentes grupos étnicos o culturales debido a diferencias en la estructura facial.

5. Privacidad y ética:

El reconocimiento facial plantea preocupaciones sobre la privacidad y el uso no ético de los datos faciales recopilados. La recopilación y el almacenamiento de datos biométricos pueden plantear riesgos para la seguridad y la privacidad de las personas.

6. Vulnerabilidad a ataques:

Los algoritmos de reconocimiento facial pueden ser vulnerables en ataques de manipulación, como el uso de imágenes falsas o técnicas de camuflaje para engañar al sistema.

7. Rendimiento en tiempo real:

Algunos algoritmos pueden ser computacionalmente intensivos, lo que puede limitar su rendimiento en tiempo real en sistemas con recursos limitados.

8. Fallos de identificación y falsas coincidencias:

Aunque los algoritmos han mejorado en la precisión, aún pueden ocurrir errores de identificación o falsas coincidencias,

lo que puede tener consecuencias negativas, especialmente en aplicaciones críticas como seguridad y vigilancia.

III. METODOLOGÍA Y DESARROLLO

Metodología Desarrollo de prototipo

Se toma como base la metodología de desarrollo de prototipo, la cual consta de 6 fases que nos permitirán llegar al objetivo:

- Fase 1: Recopilación y análisis de requisitos
- Fase 2: Construir un prototipo
- Fase 3: Evaluación inicial del usuario
- Fase 4: Refinar el prototipo
- Fase 5: Implementar el producto y mantener

A. Fase 1: Recopilación y analisis de requerimientos

El algoritmo seleccionado buscará características como: ojos, nariz, boca y contornos faciales para identificar posibles regiones faciales en la imagen.

Se empleará en él prototipo una Webcam HDFULL con resolución de video 1920x1080, una distancia de enfoque 1.5 metros y frecuencia de imagen 30fps.



Fig. 13 Webcam HDFULL

Una vez detectado un rostro, se extraen características distintivas de la imagen facial. Estas características pueden incluir la forma y posición de ojos, distancia entre ellos forma de la nariz boca, entre otros elementos.

B. Fase 2: Construir un prototipo

El lenguaje de programación a utilizar en el desarrollo del proyecto es Visual Studio Code, empleando en su diseño de la aplicación las siguientes librerías:

- **tkinter:** Es una biblioteca estándar de Python para crear interfaces gráficas de usuario (GUI) y el comando `from tkinter import *` importa todos los módulos de tkinter.
- **os:** Esta biblioteca proporciona una forma de usar funcionalidades del sistema operativo, como leer o escribir en el sistema de archivos
- **cv2:** Es la biblioteca de OpenCV para Python, se emplea para procesamiento de imágenes y visión por computadora

- **matplotlib.pyplot:** Se utiliza para crear gráficos y visualizaciones de datos.
- **MTCNN:** Es una implementación para crear una red neuronal convolucional multitarea, utilizada para detección de rostros.
- **numpy:** Proporciona soporte para matrices y operaciones matemáticas de alto nivel.

Se tomará captura del rostro, capturando video como imagen y se asignará nombre del usuario, posteriormente se exporta la imagen y se guardará en un tamaño de 150x200.

C. Interfaz

Registro de Nuevos Usuarios

Se realiza un diseño GUI con una interfaz gráfica intuitiva, para realizar el registro de manera óptima y un fácil manejo para él usuario.

```

30 def reg_rostro(img, lista_resultados):
31     data = pyplot.imread(img)
32     for i in range(len(lista_resultados)):
33         x1,y1=ancho, alto = lista_resultados[i]['box']
34         x2,y2 = x1 + ancho, y1 + alto
35         pyplot.subplot(1, len(lista_resultados), i+1)
36         pyplot.axis('off')
37         cara_reg = data[y1:y2, x1:x2]
38         cara_reg = cv2.resize(cara_reg, (150,200), interpolation = cv2.INTER_CUBIC) #Guardamos la imagen con un tamaño de 150x200
39         cv2.imwrite(usuario_img + ".jpg", cara_reg)
40         pyplot.imshow(data[y1:y2, x1:x2])
41         pyplot.show()
42
43 img = usuario_img + ".jpg"
44 pixeles = pyplot.imread(img)
45 detector = MTCNN()
46 caras = detector.detect_faces(pixeles)
47 reg_rostro(img, caras)
    
```

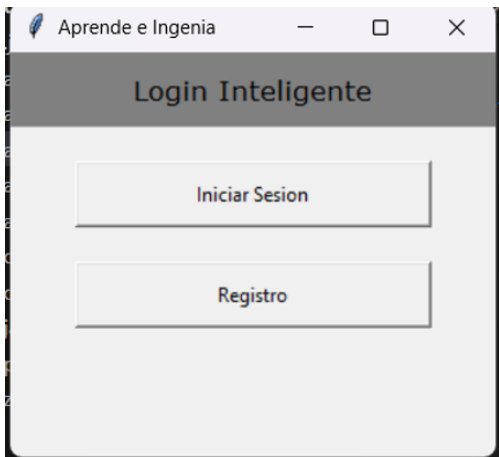


Fig. 14 Interfax FaceNet

Al presionar el botón Registro, abre la venta con dos opciones, las cuales son:

- **Registro tradicional** registro de manera manual, ingresando nombre de usuario y una contraseña.
- **Registro facial**, se activa la cámara, identifica el rostro del usuario y almacena de manera automatizada.

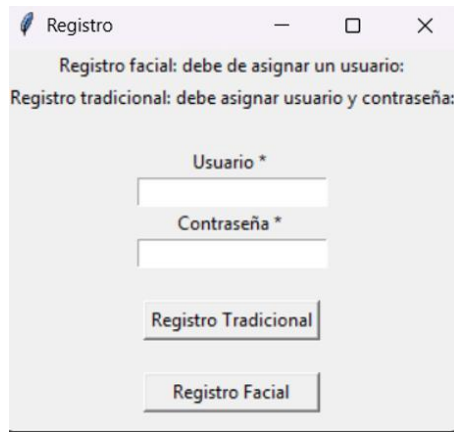


Fig. 15 Opciones de registro

Para el caso de registro fácil se registra los datos del personal como: nombre, número de empleado y tomar fotos de su rostro, con la finalidad de que FaceNet pueda reconocer al personal una vez agregado a la base de datos donde guarda los rostros de todo el personal.

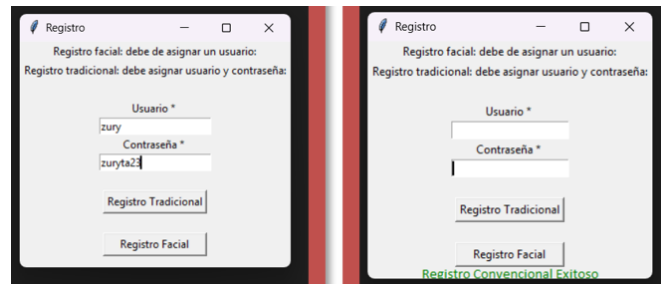


Fig. 16 Registro de datos

Al seleccionar el registro facial abre la cámara tomando foto del usuario y guardando sus datos.

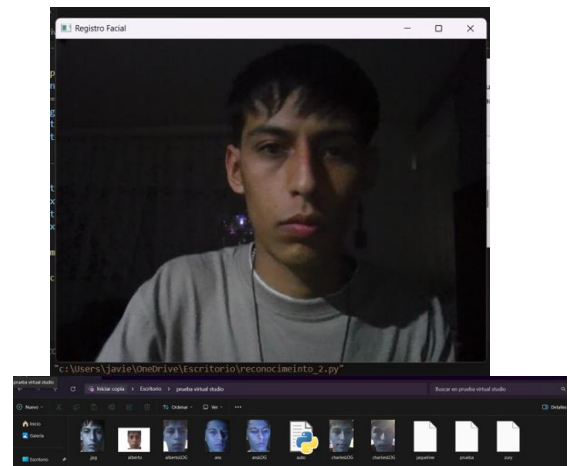


Fig. 17 Almacenan las imágenes

Estas imágenes se guardan en una carpeta exclusiva para los usuarios registrados.

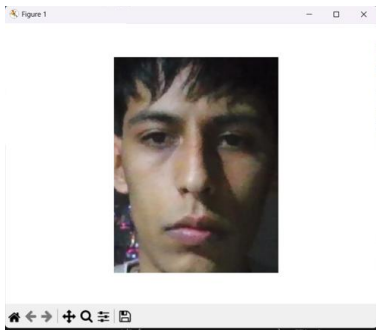


Fig. 18 Registro de rostro

Ingreso por sistema

Para el registro de entrada /salida, FaceNet tendrá dos opciones para el acceso:

- Inicio tradicional que es mediante el teclado con nombre de usuario y contraseña
- Inicio facial

Con base a la opción seleccionada FaceNet identifica de manera automatizada la identidad de la persona. Esto puede implicar una coincidencia positiva, una falta de coincidencia o un resultado incierto. Dependiendo del contexto de uso, se pueden tomar acciones específicas, como permitir el acceso, generar alertas o realizar otras operaciones relacionadas con la identificación de la persona.

Al iniciar de forma tradicional aparecerá un mensaje de salida diciendo inicio de sesión exitoso como se muestra en la Fig. 19. De lo contrario aparecerá usuario no encontrado

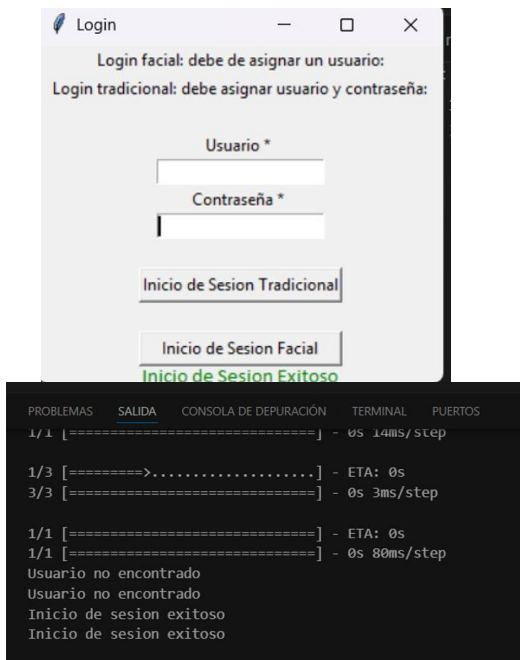


Fig. 19 Inicio de sesión exitoso

Las técnicas comunes para la extracción de características incluyen el análisis de puntos clave, el análisis de texturas y el

análisis de patrones. A partir de las características que se obtienen, se crea una representación numérica o vector que captura las características únicas del rostro. Esta representación se conoce como "plantilla facial" o "descriptores faciales" y se utiliza para realizar comparaciones al buscar similitudes en la etapa de reconocimiento, se compara la plantilla facial de la persona que se quiere identificar con las plantillas faciales almacenadas en la base de datos.

Al detectar el rostro, se ejecuta el algoritmo de coincidencia para determinar el grado de similitud o distancia entre las características faciales. Si hay una coincidencia cercana o por encima de un umbral establecido, se considera que la persona ha sido reconocida enviando mensaje de inicio de sesión exitoso de lo contrario aparece usuario no encontrado

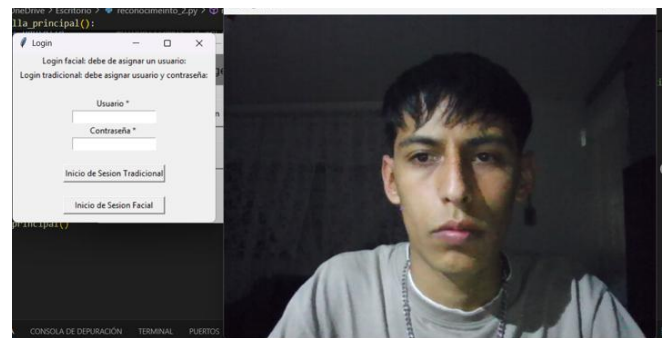


Fig. 19 Inicio de sesión

IV. CONCLUSIONES

El desarrollo de una interfaz de reconocimiento facial representa un avance significativo en la identificación y autenticación biométrica, con aplicaciones en seguridad, control de acceso, análisis de comportamiento y personalización de servicios. A lo largo de este estudio, se ha abordado la metodología necesaria para diseñar una interfaz eficiente, desde la adquisición de imágenes hasta la implementación de algoritmos avanzados de aprendizaje profundo como FaceNet.

Uno de los aspectos más importantes en este tipo de sistemas es la precisión y rapidez en la identificación de rostros, lo que requiere modelos optimizados para diferentes plataformas, ya sea en la nube, dispositivos móviles o sistemas embebidos. Además, se han identificado desafíos clave, como la variabilidad en condiciones de iluminación, la detección de intentos de suplantación y el cumplimiento de normativas de privacidad, como el Reglamento General de Protección de Datos. A pesar de sus beneficios, la implementación de una interfaz de reconocimiento facial debe considerar la ética en el manejo de datos biométricos, asegurando que la información de los usuarios esté protegida mediante cifrado y técnicas de anonimización de datos. Asimismo, es crucial seguir investigando métodos de mejora en la detección de rostros en entornos no controlados y la reducción de sesgos algorítmicos.

En conclusión, una interfaz de reconocimiento facial bien diseñada tiene el potencial de mejorar la seguridad y la experiencia del usuario en múltiples sectores.

Las recomendaciones serian implementar técnicas de reducción de ruido y normalización de imagen para mejorar la identificación facial en diferentes condiciones.

REFERENCIAS

- [1] Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D face recognition: A survey. *Pattern Recognition Letters*, 28(14), 1885–1906. <https://doi.org/10.1016/j.patrec.2006.12.018>
- [2] Deng, J., Guo, J., Xue, N., & Zafeiriou, S. (2019). ArcFace: Additive Angular Margin Loss for Deep Face Recognition. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 4690–4699. <https://doi.org/10.1109/CVPR.2019.00482>
- [3] Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep Face Recognition. *British Machine Vision Conference (BMVC)*, 41.1–41.12. <https://doi.org/10.5244/C.29.41>
- [4] Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A Unified Embedding for Face Recognition and Clustering. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 815–823. <https://doi.org/10.1109/CVPR.2015.7298682>
- [5] Taigman, Y., Yang, M., Ranzato, M., & Wolf, L. (2014). DeepFace: Closing the gap to human-level performance in face verification. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1701–1708. <https://doi.org/10.1109/CVPR.2014.220>
- [6] Turk, M., & Pentland, A. (1991). Face recognition using eigenfaces. *Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 586–591. <https://doi.org/10.1109/CVPR.1991.139758>
- [7] Woodrow, W. W. (1960). Pattern recognition and reading machines. *IRE Transactions on Information Theory*, 6(2), 54–57. <https://doi.org/10.1109/TIT.1960.1057573>
- [8] Zhang, K., Zhang, Z., Li, Z., & Qiao, Y. (2016). Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks. *IEEE Signal Processing Letters*, 23(10), 1499–1503. <https://doi.org/10.1109/LSP.2016.2603342>