

Estado del Arte de la Autenticación e Identificación de Personas por Medio del Rostro

Mena Reyes Ana Elisa
Maestría en Ciencias en Ingeniería Electrónica
Instituto Tecnológico de Morelia
Morelia, Michoacán
M19120367@morelia.tecnm.mx
Mayo 2026

Resumen— La autenticación e identificación de personas mediante reconocimiento facial se ha convertido en una de las tecnologías biométricas más utilizadas en la actualidad debido a su precisión y facilidad de uso. Esta tecnología emplea algoritmos de visión por computadora, aprendizaje automático e inteligencia artificial para analizar las características faciales de cada persona y compararlos con bases de datos previamente registradas [11]. En los últimos años, el avance de las redes neuronales profundas y el incremento de la capacidad computacional han permitido desarrollar sistemas capaces de alcanzar altos niveles de exactitud, incluso si las personas hacen gestos o se encuentran en un lugar con poca iluminación [7], [14].

El presente artículo analiza el estado del arte de las técnicas modernas de autenticación e identificación facial, describiendo las principales etapas del reconocimiento facial, los algoritmos clásicos y los modernos, así como las herramientas y los marcos de trabajo (frameworks) utilizados actualmente en aplicaciones académicas y comerciales. También se revisan las características biométricas que distinguen un rostro de otro, las bases de datos más utilizadas para entrenamiento y evaluación, así como las ventajas y las limitaciones de esta tecnología.

Palabras clave— reconocimiento facial, biometría, autenticación facial, identificación facial, inteligencia artificial, redes neuronales convolucionales.

I. INTRODUCCIÓN

El reconocimiento facial es una técnica biométrica que permite identificar personas a partir de las características que poseen sus rostros. El término biometría hace referencia al uso de las características físicas y de conducta que tiene cada persona para poder reconocerla [10]. Entre las tecnologías biométricas más comunes se encuentran las huellas dactilares, el reconocimiento de iris, la voz y el reconocimiento facial.

Actualmente, el reconocimiento facial tiene aplicaciones en múltiples áreas como control de acceso, dispositivos móviles, vigilancia, seguridad pública, redes sociales, etc. Las grandes empresas tecnológicas como Apple, Google y Microsoft también han incorporado esta tecnología en sus dispositivos y servicios, mientras que los gobiernos y las organizaciones

la utilizan en ciertos puntos de la ciudad en los sistemas de monitoreo y la autenticación digital.

El crecimiento de esta tecnología se debe principalmente al desarrollo de las técnicas de inteligencia artificial y aprendizaje profundo (Deep Learning), y especialmente a las Redes Neuronales Convolucionales (CNN), que han demostrado un rendimiento superior comparado con otros métodos [9], [15].

Sin embargo, el uso de estas tecnologías también se ha relacionado mucho con la privacidad, la vigilancia de las personas y la protección de datos.

II. CONCEPTOS FUNDAMENTALES

A. Biometría

La biometría consiste en medir y analizar características biológicas o conductuales de una persona para verificar su identidad. Las características biométricas deben cumplir los siguientes requisitos:

- Universalidad.
- Singularidad.
- Permanencia.
- Medibilidad.
- Rendimiento.
- Aceptabilidad.

El rostro humano cumple gran parte de estos requisitos, ya que presenta características únicas y relativamente estables a lo largo del tiempo [11].

B. Diferencia entre autenticación e identificación

La autenticación facial verifica si una persona es quien afirma ser. Este proceso generalmente se realiza comparando el rostro capturado con una sola plantilla almacenada.

La identificación facial busca determinar quién es una persona dentro de una base de datos que contiene múltiples identidades registradas [28].

C. Reconocimiento facial

El reconocimiento facial es el proceso automatizado que detecta, analiza y compara rostros humanos utilizando algoritmos computacionales [10]. El proceso, sigue los siguientes pasos:

- Captura de imagen.
- Detección del rostro.
- Extracción de características.
- Generación de representación matemática.
- Comparación con bases de datos.
- Decisión de autenticación o identificación.

III. CARACTERÍSTICAS BIOMÉTRICAS DEL ROSTRO

El rostro humano posee múltiples puntos y patrones característicos que permiten diferenciar a una persona de otra. Los sistemas modernos analizan una combinación de geometría facial, textura y relaciones espaciales [10].

A. Puntos característicos

Los algoritmos de reconocimiento facial suelen detectar puntos faciales clave, como:

- Distancia entre los ojos.
- Ancho de la nariz.
- Forma del mentón.
- Posición de pómulos.
- Contorno de labios.
- Forma de cejas.
- Distancia entre la nariz y la boca.
- Estructura de la mandíbula.

Estos puntos permiten construir una representación matemática única conocida como embedding facial, **Li y Jain** [10].

B. Geometría facial

La geometría facial estudia las relaciones espaciales entre los distintos puntos del rostro. Cada persona tiene proporciones faciales distintas que ayudan a distinguirla de otra.

C. Textura facial

La textura facial incluye los patrones de la piel, arrugas, líneas de expresión y detalles superficiales. Las técnicas modernas utilizan mapas de textura para mejorar la precisión.

D. Características tridimensionales

Los sistemas avanzados utilizan sensores 3D para capturar la profundidad y la estructura facial de las personas. Esto

ayuda a reducir los errores producidos por la iluminación o el uso de fotografías falsas.

IV. ETAPAS DE UN SISTEMA DE RECONOCIMIENTO FACIAL

A. Adquisición de imágenes

La primer etapa consiste en capturar la imagen o video de la persona mediante cámaras digitales, cámaras infrarrojas o sensores de profundidad.

La calidad de captura influye directamente en el sistema que se maneje. Los factores como la iluminación, resolución, movimiento y ángulo afectan la precisión de la captura [13].

B. Detección facial

La detección facial localiza automáticamente el rostro dentro de una imagen. Los métodos clásicos de detección son los siguientes:

1) Viola-Jones

El algoritmo Viola-Jones fue uno de los primeros métodos exitosos de detección facial en tiempo real [3]. Utiliza:

- Características Haar.
- Imágenes integrales.
- Clasificadores AdaBoost.
- Cascadas de clasificación.

Sus ventajas son la rapidez y simplicidad, aunque presenta limitaciones en poses más complejas.

2) Histogram of Oriented Gradients (HOG)

El método HOG describe la distribución de gradientes en una imagen para detectar objetos y rostros [33].

Métodos modernos

Actualmente se utilizan redes neuronales profundas como:

- MTCNN (Multi-task Cascaded Convolutional Neural Networks) [16].
- RetinaFace [17].
- YOLO Face [18].
- SSD Face Detector [19].

Estos modelos presentan un mejor rendimiento en diferentes condiciones de iluminación y pose.

C. Alineación facial

La alineación facial ajusta el rostro para normalizar orientación, tamaño y posición de ojos y boca.

Esta etapa mejora considerablemente el rendimiento del reconocimiento [13].

D. Extracción de características

La extracción de características transforma el rostro en un vector numérico representativo.

Métodos tradicionales

- Eigenfaces.
- Fisherfaces.
- Local Binary Patterns Histograms (LBPH).
- Principal Component Analysis (PCA).
- Linear Discriminant Analysis (LDA) [2].

Métodos basados en Deep Learning

Las CNN aprenden automáticamente características discriminantes a partir de grandes conjuntos de datos [7].

E. Comparación y clasificación

Los vectores faciales se comparan utilizando métricas matemáticas como:

- Distancia euclidiana.
- Similitud coseno.
- Distancia Manhattan.

Posteriormente se toma una decisión basada en umbrales de similitud.

V. ALGORITMOS Y TÉCNICAS ACTUALES

A. Eigenfaces

Eigenfaces (o "Caras Propias"), fue uno de los primeros métodos de reconocimiento facial. Este método utiliza el PCA (Análisis de Componentes Principales, en español) para reducir la dimensionalidad y representar los rostros mediante vectores propios [2], [29].

El PCA es un método estadístico y matemático (basado en álgebra lineal) cuyo objetivo principal es la reducción de la dimensionalidad de un conjunto de datos, perdiendo la menor cantidad de información posible.

Ventajas

- Simplicidad.
- Bajo costo computacional.
- Fácil implementación.

Desventajas

Sensible a iluminación.
Bajo desempeño en variaciones faciales.

B. Fisherfaces

Fisherfaces fue la evolución directa de *Eigenfaces*. Surgió para resolver el problema que tenía el método anterior: los cambios drásticos de iluminación y las expresiones faciales

[29]. Este método utiliza el Análisis Discriminante Lineal (LDA) para maximizar la separación entre clases faciales.

C. LBPH

Local Binary Patterns Histograms (Histogramas de Patrones Binarios Locales) analiza texturas locales del rostro. A diferencia de Eigenfaces y Fisherfaces, que analiza la imagen de forma global (matemáticas aplicadas a toda la matriz de la foto), LBPH adopta un enfoque local [27]. Esto significa que analiza la imagen pixel por pixel y sección por sección, enfocándose en la textura del rostro.

Ventajas

Buen desempeño en tiempo real.
Menor sensibilidad a iluminación.
Fácil implementación.

Desventajas

Menor precisión comparado con Deep Learning.

D. Redes Neuronales Convolucionales (CNN)

Las CNN revolucionaron el reconocimiento facial debido a su capacidad para aprender características automáticamente. Son un tipo de inteligencia artificial especializada en analizar imágenes y video [7]. Son la base de la mayoría de los sistemas modernos de reconocimiento facial. Las CNN automatizan la extracción de caracteres mediante entrenamiento, determinan los píxeles y las formas más importantes para reconocer un rostro.

E. DeepFace

DeepFace es un sistema de reconocimiento facial basado en redes neuronales convolucionales desarrollado por Meta en 2014. Este modelo introdujo técnicas avanzadas de alineación facial tridimensional y aprendizaje profundo para extraer representaciones biométricas altamente discriminativas. DeepFace logró una precisión cercana al nivel humano en tareas de verificación facial, marcando un punto de referencia en la evolución de los sistemas modernos de reconocimiento facial [5], [11].

F. FaceNet

FaceNet es un modelo de reconocimiento facial desarrollado por Google que utiliza redes neuronales convolucionales para generar embeddings faciales compactos y altamente discriminativos. Su principal contribución fue la introducción de la función Triplet Loss, la cual optimiza la distancia entre representaciones faciales de individuos iguales y diferentes [4].

G. ArcFace

ArcFace es un modelo avanzado de reconocimiento facial también basado en redes neuronales convolucionales que introduce una función de pérdida angular aditiva para mejorar la separación entre embeddings faciales. Esta arquitectura incrementa significativamente la capacidad discriminativa del

sistema, permitiendo altos niveles de precisión en tareas de autenticación e identificación biométrica. Debido a su rendimiento superior, ArcFace es actualmente uno de los modelos más utilizados en sistemas modernos de reconocimiento facial [6].

H. VGGFace y VGGFace2

VGGFace es un modelo de reconocimiento facial basado en redes neuronales desarrollado por el Visual Geometry Group de la Universidad de Oxford. Su arquitectura profunda permite extraer automáticamente características faciales discriminativas para tareas de autenticación e identificación biométrica.

Posteriormente, VGGFace2 amplió este trabajo mediante la creación de un dataset facial de gran escala con alta variabilidad en poses, edades e iluminación, permitiendo entrenar modelos más robustos y precisos para aplicaciones modernas de reconocimiento facial [5].

VI. HERRAMIENTAS Y FRAMEWORKS UTILIZADOS ACTUALMENTE

A. OpenCV

OpenCV es una biblioteca de visión por computadora ampliamente utilizada para procesamiento de imágenes y reconocimiento facial [12].

Funcionalidades

- Detección facial.
- Procesamiento de imágenes.
- Reconocimiento en tiempo real.
- Integración con cámaras.

B. Dlib

Dlib es una biblioteca de código abierto especializada en aprendizaje automático y visión por computadora. Proporciona herramientas avanzadas para detección facial, extracción de landmarks y generación de embeddings faciales mediante redes neuronales profundas [8]. Debido a su precisión y facilidad de integración con Python y OpenCV, Dlib es ampliamente utilizada en sistemas biométricos de autenticación e identificación facial.

C. TensorFlow

TensorFlow permite desarrollar y entrenar modelos de Deep Learning. Es un framework de aprendizaje profundo desarrollado por Google utilizado en sistemas de reconocimiento facial y visión por computadora. Su arquitectura permite entrenar redes neuronales de alta complejidad, facilitando tareas de autenticación biométrica, clasificación facial y generación de embeddings faciales [20].

D. PyTorch

PyTorch es un framework de aprendizaje profundo desarrollado por Meta que proporciona herramientas flexibles

para el diseño y entrenamiento de redes neuronales profundas. Debido a su arquitectura dinámica y facilidad de experimentación, PyTorch se utiliza en la investigación de reconocimiento facial y modelos avanzados de inteligencia artificial [21].

E. Face Recognition Library

Face Recognition Library es una biblioteca de Python especializada en reconocimiento facial basada en Dlib y redes neuronales convolucionales [13]. Esta herramienta permite implementar sistemas biométricos de autenticación facial mediante detección de rostros, extracción de embeddings y comparación de características faciales.

F. MediaPipe

MediaPipe es un framework desarrollado por Google para procesamiento multimedia y visión por computadora en tiempo real [22]. Su módulo Face Mesh permite detectar cientos de landmarks faciales tridimensionales, facilitando aplicaciones de seguimiento facial, realidad aumentada y autenticación biométrica en dispositivos móviles y sistemas interactivos.

G. Azure Face API

Azure Face API es un servicio de reconocimiento facial basado en la nube desarrollado por Microsoft. Esta plataforma proporciona herramientas de detección, verificación e identificación facial mediante inteligencia artificial, permitiendo integrar sistemas biométricos escalables en aplicaciones empresariales y servicios digitales [23].

H. AWS Rekognition

AWS Rekognition es un servicio de análisis visual basado en inteligencia artificial desarrollado por Amazon Web Services [24]. Esta plataforma permite implementar sistemas de reconocimiento facial, detección de personas y análisis automatizado de imágenes y video mediante infraestructura escalable en la nube.

VII. BASES DE DATOS UTILIZADAS EN RECONOCIMIENTO FACIAL

A. Labeled Faces in the Wild (LFW)

Labeled Faces in the Wild (LFW) es una de las bases de datos más utilizadas para evaluar sistemas de reconocimiento facial. Contiene más de 13,000 imágenes de rostros obtenidas en condiciones reales y no controladas [11], incluyendo variaciones de iluminación, pose y expresiones faciales. Este dataset ha sido ampliamente como estándar de referencia para medir la precisión de modelos biométricos y algoritmos de deep learning.

B. CASIA-WebFace

CASIA-WebFace es una base de datos desarrollada para el entrenamiento de modelos de reconocimiento facial

basados en aprendizaje profundo. Contiene aproximadamente 500,000 imágenes correspondientes a más de 10,000 personas diferentes. Debido a su tamaño y diversidad facial, es bastante utilizada en el entrenamiento de redes neuronales convolucionales y sistemas modernos de autenticación biométrica [25].

C. VGGFace2

VGGFace2 es una base de datos facial desarrollada por la Universidad de Oxford que contiene millones de imágenes con gran variabilidad en edad, iluminación, expresiones y pose [5]. Su principal objetivo es entrenar modelos robustos capaces de reconocer personas bajo diferentes condiciones faciales y ambientales.

D. MS-Celeb-1M

Es una base de datos creada por Microsoft que contiene millones de imágenes faciales de miles de individuos. Fue diseñada para el entrenamiento masivo de modelos de deep learning y permitió mejorar la precisión de los sistemas modernos de reconocimiento facial. Sin embargo, también generó ciertas controversias relacionadas con la privacidad y el uso ético de datos biométricos [26].

E. FERET

Es de las bases de datos clásicas más importantes en investigación biométrica facial. Fue desarrollada para evaluar algoritmos tempranos de reconocimiento facial en ambientes controlados [10]. Aunque actualmente existen datasets más avanzados, FERET continúa siendo una referencia histórica en el desarrollo y comparación de técnicas biométricas.

VIII. APLICACIONES ACTUALES

A. Dispositivos móviles

Los teléfonos inteligentes utilizan reconocimiento facial para desbloqueo y autenticación.

B. Seguridad y vigilancia

Los sistemas de videovigilancia emplean reconocimiento facial para detectar personas de interés.

C. Control de acceso

Empresas y edificios utilizan autenticación facial para restringir acceso.

D. Sistemas bancarios

Los bancos usan reconocimiento facial para validar las identidades.

E. Redes sociales

Las plataformas sociales etiquetan automáticamente personas en fotografías.

F. Salud

En medicina se investiga el reconocimiento facial para detectar enfermedades genéticas.

G. Comercio electrónico

Se utiliza para pagos biométricos y autenticación de usuarios [30].

IX. VENTAJAS DEL RECONOCIMIENTO FACIAL

- No requiere contacto físico.
- Proceso rápido y automatizado.
- Fácil integración con cámaras existentes.
- Alta comodidad para usuarios.
- Permite autenticación remota.
- Mejora sistemas de seguridad.
- Compatible con inteligencia artificial.

X. LIMITACIONES Y PROBLEMAS ACTUALES

A. Variaciones de iluminación

Los cambios de iluminación afectan significativamente la precisión.

B. Oclusiones

Mascarillas, lentes y accesorios pueden dificultar el reconocimiento.

C. Cambios de pose

Los rostros vistos desde ángulos extremos generan errores.

D. Envejecimiento

El paso del tiempo modifica características faciales.

E. Ataques de suplantación

Fotografías, videos y máscaras pueden engañar sistemas inseguros.

F. Sesgos algorítmicos

Algunos sistemas presentan menor precisión en determinados grupos poblacionales.

G. Privacidad

El almacenamiento de datos biométricos genera preocupaciones legales y éticas [31].

XI. TÉCNICAS DE SEGURIDAD Y ANTI-SPOOFING

Los sistemas modernos incluyen mecanismos para detectar intentos de fraude [32].

A. Detección de vida (Liveness Detection)

Verifica que el rostro pertenezca a una persona real y no a una fotografía.

Métodos utilizados

- Parpadeo.
- Movimiento facial.
- Profundidad 3D.
- Análisis térmico.
- Reflexión de luz.

B. Reconocimiento 3D

Los sensores de profundidad ayudan a evitar ataques mediante imágenes planas.

C. Análisis multiespectral

Utiliza información infrarroja y térmica para validar autenticidad.

XII. INTELIGENCIA ARTIFICIAL Y DEEP LEARNING

La inteligencia artificial ha impulsado enormemente el reconocimiento facial [7].

A. Aprendizaje supervisado

Los modelos se entrenan con imágenes etiquetadas.

B. Aprendizaje profundo

Las redes neuronales profundas aprenden automáticamente patrones complejos.

C. Transfer Learning

Permite reutilizar modelos previamente entrenados.

D. Transformers y Vision Transformers (ViT)

Las arquitecturas basadas en transformers están comenzando a utilizarse en visión por computadora.

XIII. COMPARACIÓN ENTRE MÉTODOS TRADICIONALES Y MODERNOS

Características	Métodos Tradicionales	Métodos Modernos
Presición	Media	Muy alta
Requerimiento computacional	Bajo	Alto
Robustez	Limitada	Alta
Sensibilidad a iluminación	Alta	Menor
Adaptabilidad	Baja	Alta
Tiempo de entrenamiento	Corto	Largo

Los métodos modernos basados en Deep Learning dominan actualmente debido a su capacidad para manejar escenarios complejos [34].

XIV. ASPECTOS ÉTICOS Y LEGALES

A. Privacidad

El reconocimiento facial puede utilizarse para vigilancia masiva.

B. Consentimiento

Es importante que las personas conozcan cuándo sus datos biométricos son utilizados.

C. Protección de datos

Las bases de datos faciales deben almacenarse de forma segura.

D. Regulaciones

Diversos países han comenzado a regular el uso de biometría facial.

E. Sesgo y discriminación

Es necesario desarrollar modelos equilibrados y representativos [35].

XV. TENDENCIAS FUTURAS

Las investigaciones actuales buscan mejorar precisión, seguridad y eficiencia [30], [35].

A. Reconocimiento multimodal

Combina rostro con voz, iris u otras biometrías.

B. Edge Computing

Permite ejecutar reconocimiento facial directamente en dispositivos locales.

C. Federated Learning

Entrena modelos sin compartir datos sensibles.

D. IA explicable

Busca entender cómo toman decisiones los modelos de inteligencia artificial.

E. Integración con realidad aumentada

El reconocimiento facial será utilizado en sistemas inmersivos y metaverso.

XVI. DISCUSIÓN

El reconocimiento facial ha evolucionado desde métodos estadísticos simples hasta complejos modelos de inteligencia artificial capaces de superar niveles de precisión humana en ciertos escenarios. El Deep Learning transformó esta área gracias a las CNN y modelos avanzados como FaceNet y ArcFace.

Sin embargo, todavía existen aspectos importantes relacionados con privacidad, seguridad y sesgo algorítmico que hay que mejorar. La necesidad de sistemas más transparentes y éticos será fundamental en el futuro.

Además, el crecimiento de dispositivos inteligentes y ciudades conectadas continuará impulsando el uso e implementación de estas tecnologías en múltiples sectores.

XVII. CONCLUSIONES

La autenticación e identificación de personas mediante reconocimiento facial representa una de las áreas más importantes de la biometría moderna. Los avances en inteligencia artificial y aprendizaje profundo han permitido desarrollar sistemas bastante precisos y robustos.

Actualmente, las técnicas basadas en redes neuronales convolucionales dominan el estado del arte debido a su capacidad para extraer automáticamente características faciales discriminantes y adaptarse a condiciones complejas.

REFERENCIAS

- [1] R. Chellappa, C. Wilson y S. Sirohey, "Human and machine recognition of faces: A survey," *Proceedings of the IEEE*, vol. 83, no. 5, pp. 705-741, 1995. DOI: 10.1109/5.381842
- [2] M. Turk y A. Pentland, "Eigenfaces for recognition," *Journal of Cognitive Neuroscience*, vol. 3, no. 1, pp. 71-86, 1991. DOI: 10.1162/jocn.1991.3.1.71
- [3] P. Viola y M. Jones, "Rapid object detection using a boosted cascade of simple features," *IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2001. DOI: 10.1109/CVPR.2001.990517
- [4] F. Schroff, D. Kalenichenko y J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," *IEEE Conference on Computer Vision and Pattern Recognition*, 2015. DOI: 10.1109/CVPR.2015.7298682
- [5] O. M. Parkhi, A. Vedaldi y A. Zisserman, "Deep Face Recognition," *British Machine Vision Conference*, 2015. DOI: 10.5244/C.29.41
- [6] J. Deng et al., "ArcFace: Additive angular margin loss for deep face recognition," *IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019. DOI: 10.1109/CVPR.2019.00482
- [7] I. Goodfellow, Y. Bengio y A. Courville, *Deep Learning*. MIT Press, 2016. URL: <http://www.deeplearningbook.org>
- [8] D. King, "Dlib-ml: A machine learning toolkit," *Journal of Machine Learning Research*, vol. 10, pp. 1755-1758, 2009. URL: <https://www.jmlr.org/papers/v10/king09a.html>
- [9] A. Krizhevsky, I. Sutskever y G. Hinton, "ImageNet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, 2012. DOI: 10.1145/3065386
- [10] S. Z. Li y A. Jain, *Handbook of Face Recognition*. Springer, 2011. DOI: 10.1007/978-0-85729-932-1
- [11] Y. Taigman et al., "DeepFace: Closing the gap to human-level performance in face verification," *IEEE Conference on Computer Vision and Pattern Recognition*, 2014. DOI: 10.1109/CVPR.2014.220
- [12] G. Bradski, "The OpenCV Library," *Dr. Dobb's Journal of Software Tools*, 2000. URL: <https://www.drdobbs.com/open-source/the-opencv-library/184404319>
- [13] A. Geitgey, *Face Recognition Library Documentation*, 2020. URL: https://github.com/ageitgey/face_recognition
- [14] K. He, X. Zhang, S. Ren y J. Sun, "Deep residual learning for image recognition," *IEEE Conference on Computer Vision and Pattern Recognition*, 2016. DOI: 10.1109/CVPR.2016.90
- [15] A. Vaswani et al., "Attention is all you need," *Advances in Neural Information Processing Systems*, 2017. URL: <https://arxiv.org/abs/1706.03762>
- [16] K. Zhang, Z. Zhang, Z. Li y Y. Qiao, "Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks," *IEEE Signal Processing Letters*, vol. 23, no. 10, pp. 1499-1503, 2016. DOI: 10.1109/LSP.2016.2603342
- [17] J. Deng, J. Guo, E. Ververas, I. Kotsia y S. Zafeiriou, "RetinaFace: Single-Shot Multi-Level Face Localisation in the Wild," *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020, pp. 5203-5212. DOI: 10.1109/CVPR42600.2020.00525
- [18] W. Chen, P. Huang, J. Peng, Q. Wu y R. Zhang, "YOLOface: A Real-Time Face Detector," *The Visual Computer*, vol. 37, pp. 805-813, 2021. DOI: 10.1007/s00371-020-01831-7
- [19] W. Liu, D. Anguelov, D. Erhan, C. Szegedy, S. Reed, C. Y. Fu y A. C. Berg, "SSD: Single shot multibox detector," *European Conference on Computer Vision (ECCV)*, 2016, pp. 21-37. DOI: 10.1007/978-3-319-46448-0_2
- [20] M. Abadi et al., "TensorFlow: A System for Large-Scale Machine Learning," *12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, 2016, pp. 265-283. DOI: 10.5555/3026877.3026899
- [21] A. Paszke et al., "PyTorch: An Imperative Style, High-Performance Deep Learning Library," *Advances in Neural Information Processing Systems (NeurIPS)*, vol. 32, 2019, pp. 8024-8035. URL: <https://proceedings.neurips.cc/paper/2019/hash/bdbca288fee7f92f2bfa9f7012727740-Abstract.html>
- [22] C. Lugaresi et al., "MediaPipe: A Framework for Building Perception Pipelines," *arXiv preprint*

arXiv:1906.08172, 2019. DOI:
10.48550/arXiv.1906.08172

- [23] Microsoft Azure, "Face documentation - Azure AI services," 2023. [En línea]. Disponible en: <https://learn.microsoft.com/en-us/azure/ai-services/computer-vision/overview-identity>
- [24] Amazon Web Services, "Amazon Rekognition Developer Guide," 2023. [En línea]. Disponible en: <https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html>
- [25] D. Yi, Z. Lei, S. Liao y S. Z. Li, "Learning Face Representation from Scratch," arXiv preprint arXiv:1411.7923, 2014. DOI: 10.48550/arXiv.1411.7923
- [26] Y. Guo, L. Zhang, Y. Hu, X. He y J. Gao, "MS-Celeb-1M: A Dataset and Benchmark for Large-Scale Face Recognition," European Conference on Computer Vision (ECCV), 2016, pp. 87-102. DOI: 10.1007/978-3-319-46487-9_6
- [27] T. Ahonen, A. Hadid y M. Pietikäinen, "Face Description with Local Binary Patterns: Application to Face Recognition," IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), vol. 28, no. 12, pp. 2037-2041, 2006. DOI: 10.1109/TPAMI.2006.244
- [28] ISO/IEC, "Information technology — Biometrics — Vocabulary," ISO/IEC 2382-37:2022, 2022. [En línea]. Disponible en: <https://www.iso.org/standard/79521.html>
- [29] P. N. Belhumeur, J. P. Hespanha y D. J. Kriegman, "Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection," IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI), vol. 19, no. 7, pp. 711-720, 1997. DOI: 10.1109/34.598228
- [30] I. Adjabi, A. Ouahabi, A. Benzaoui y A. Taleb-Ahmed, "Past, Present, and Future of Face Recognition: A Review," Electronics, vol. 9, no. 8, p. 1188, 2020. DOI: 10.3390/electronics9081188
- [31] M. J. Thorpe, "Challenges in Facial Recognition: A Review of Illumination, Pose, and Occlusion Issues," Journal of Cybersecurity and Privacy, vol. 2, no. 1, pp. 45-62, 2022. DOI: 10.3390/jcp2010004
- [32] S. Ramachandra y C. Busch, "Presentation Attack Detection Methods for Face Recognition Systems: A Comprehensive Survey," ACM Computing Surveys, vol. 50, no. 1, pp. 1-37, 2017. DOI: 10.1145/3038675
- [33] N. Dalal y B. Triggs, "Histograms of Oriented Gradients for Human Detection," IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR), 2005, pp. 886-893. DOI: 10.1109/CVPR.2005.177
- [34] A. S. Tolba, A. H. El-Baz y A. A. El-Harby, "Face Recognition: A Comparative Study," International Journal of Computer Science and Network Security, vol. 6, no. 1, pp. 41-53, 2006.
- [35] O. M. Parkhi, A. Vedaldi y A. Zisserman, "Deep Face Recognition," Proceedings of the British Machine Vision Conference (BMVC), 2015, pp. 41.1-41.12. DOI: 10.5244/C.29.41